



АйТи Мониторинг
ЗАЩИТА ИНФОРМАЦИИ

УТВЕРЖДАЮ
Управляющий
ООО «АйТи Мониторинг»
/С.И. Крецу
«20» сентября 2024 г.

М.П.

**Порядок реализации функций
аккредитованного удостоверяющего центра
ООО «АйТи Мониторинг»
и исполнения его обязанностей**

г. Краснодар
2024 год



1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	4
2. ОБЩИЕ ПОЛОЖЕНИЯ	5
2.1. Предмет регулирования	5
2.2. Сведения об Удостоверяющем центре.....	6
2.3. Порядок информирования о предоставлении услуг УЦ	7
2.4. Стоимость услуг.....	7
3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ).....	7
4. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	8
4.1. Права удостоверяющего центра	8
4.2. Обязанности удостоверяющего центра	8
4.3. Права заявителя и владельца сертификата	10
4.4. Обязанности заявителя и владельца сертификата	11
5. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ) НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ.....	11
5.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей	11
5.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей... 11	11
5.1.2. Порядок и сроки смены ключей электронной подписи Удостоверяющего центра	12
5.1.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности.....	12
5.1.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца сертификата.....	13
5.2. Процедура создания и выдачи Сертификатов.....	13
5.2.1. Порядок подачи заявления на создание и выдачу Сертификатов.....	13
5.2.2. Требования к заявлению на создание и выдачу Сертификатов.....	13
5.2.3. Порядок идентификации заявителя.....	14
5.2.4. Перечень документов для создания и выдачи Сертификатов	15
5.2.5. Порядок проверки достоверности документов и сведений, предоставленных заявителем.....	15
5.2.6. Порядок создания Сертификата	15
5.2.7. Порядок выдачи Сертификата	16
5.2.8. Сроки создания и выдачи Сертификата.....	16
5.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов	16
5.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата.....	17
5.4.1. Основания прекращения действия или аннулирования Сертификата.....	17
5.4.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) сертификата	17



5.5.	Порядок ведения реестра Сертификатов	18
5.6.	Порядок технического обслуживания Реестра сертификатов	19
6.	ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	19
6.1.	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	19
6.2.	Обеспечение актуальности информации, содержащейся в Реестре сертификатов, и ее защиты ..	19
6.3.	Обеспечение доступности Реестра сертификатов	19
6.4.	Обеспечение конфиденциальности созданных УЦ ключей электронных подписей	20
6.5.	Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации	20
7.	ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	20
7.1.	Подтверждение владения ключом ЭП, соответствующим сертификату ключа проверки ЭП.....	20
7.2.	Предоставление сервисов Службы актуальных статусов сертификатов и Службы штампов времени	20



1. Термины и определения

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) – физическое лицо, которому в установленном Федеральным законом № 63-ФЗ от 06.04.2011 г. «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи;

Заявитель – физическое лицо, обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата. Заявитель после создания сертификата становится владельцем сертификата;

Квалифицированный сертификат ключа проверки электронной подписи (сертификат) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом № 63-ФЗ от 06.04.2011 г. «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи;

Ключ проверки электронной подписи (ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Служба актуальных статусов сертификатов – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого подписываются квалифицированной электронной подписью и предоставляются электронные ответы, содержащие информацию о статусе сертификатов, выданных Удостоверяющим центром.

Служба штампов времени – сервис Удостоверяющего центра (построенный на базе протокола TSP), с использованием которого подписываются квалифицированной электронной подписью и предоставляются штампы времени.

Средства электронной подписи – средства криптографической защиты информации (СКЗИ), используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

Список аннулированных (отозванных) сертификатов – электронный документ с квалифицированной электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы, действие которых прекращено.

Удостоверяющий центр (УЦ) – в рамках настоящего Порядка аккредитованный удостоверяющий центр ООО «АйТи Мониторинг», осуществляющий в соответствии с Федеральным законом РФ № 63-ФЗ от 06.04.2011 «Об электронной подписи» функции по созданию и выдаче сертификатов ключей проверки

квалифицированных электронных подписей, а также иные функции, предусмотренные действующим законодательством;

Уполномоченное лицо Удостоверяющего центра (уполномоченное лицо УЦ) – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по подписанию сертификатов ключей проверки электронных подписей и списков отозванных сертификатов в электронной форме.

Электронная подпись (ЭП) – 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;

Электронный образ – подписанная квалифицированной электронной подписью владельца сертификата скан-копия оригинала документа (заявления на выдачу сертификата), созданная УЦ или доверенным лицом УЦ в системе УЦ.

2. Общие положения

2.1. Предмет регулирования

Настоящий Порядок реализации функций аккредитованного удостоверяющего центра ООО «АйТи Мониторинг» и исполнения его обязанностей (далее – Порядок), определяет порядок реализации функций аккредитованного удостоверяющего центра ООО «АйТи Мониторинг» и исполнения его обязанностей, в том числе порядок и условия предоставления услуг по выдаче и управлению сертификатами ключей квалифицированной электронной подписи, а также права, обязанности, ответственность Удостоверяющего центра и лиц, присоединившихся к данному Порядку.

С момента регистрации заявления на выдачу сертификата заинтересованное лицо считается присоединившемся в силу статьи 428 Гражданского кодекса Российской Федерации к настоящему Порядку и публичному договору на оказание услуг Удостоверяющего центра, размещенному в сети Интернет по адресу <https://e-signature.pro/documents/>, и является Стороной Порядка.

Факт присоединения лица к Порядку является полным принятием им условий настоящего Порядка и всех его приложений в редакции, действующей на момент регистрации заявления на выдачу сертификата. Лицо, присоединившееся к Порядку, принимает дальнейшие изменения, вносимые в Порядок, в соответствии с условиями настоящего Порядка.

Прекращение действия Порядка не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Порядка, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

Настоящим Стороны соглашаются с тем, что внесение изменений (дополнений) в Порядок, включая приложения к нему, осуществляется Удостоверяющим Центром в одностороннем порядке.

Информирование сторон Порядка о внесении изменений (дополнений) в Порядок осуществляется Удостоверяющим Центром путем обязательного размещения указанных изменений на официальном сайте УЦ в сети «Интернет», в том числе посредством публикации новой редакции Порядка.

Все изменения (дополнения), вносимые Удостоверяющим Центром в Порядок, не связанные с изменением законодательства Российской Федерации, вступают в силу и становятся обязательными на следующий день после дня размещения указанных изменений в Порядок на официальном сайте УЦ в сети «Интернет», если иной срок не указан в самом Порядке.



Все изменения, вносимые Удостоверяющим Центром в Порядок в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных нормативно-правовых актах.

Любые изменения и дополнения, внесенные Удостоверяющим Центром в Порядок, с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Порядку, в том числе присоединившихся к Порядку ранее даты вступления изменений в силу.

Все приложения к настоящему Порядку являются его составной и неотъемлемой частью.

После присоединения к Порядку Удостоверяющий центр и Сторона, присоединившаяся к Порядку, вступают в соответствующие договорные отношения на неопределённый срок.

Настоящий Порядок вступает в силу со дня его публикации на официальном сайте УЦ в сети Интернет и действует до прекращения деятельности Удостоверяющего Центра, либо до приятия Удостоверяющим центром Порядка в новой редакции.

2.2. Сведения об Удостоверяющем центре

ООО «АйТи Мониторинг» зарегистрировано на территории Российской Федерации в г. Краснодаре (свидетельство о государственной регистрации юридического лица серия 23 № 009257685, выдано 04 марта 2015 г. Инспекцией Федеральной налоговой службы №2 по г. Краснодару), внесено в Единый государственный реестр юридических лиц за основным государственным регистрационным номером 1152311003305.

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании решения Правительственной комиссии, уполномоченной на принятие решения об аккредитации удостоверяющих центров (протокол от 13.12.2021 № 11) и лицензии Управления ФСБ России по Краснодарскому краю от 15.04.2022 г. рег. № Л051-00105-23/00145566 на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Информация о месте нахождения и графике работы УЦ:

Полное наименование: Общество с ограниченной ответственность «АйТи Мониторинг»

Адрес места нахождения: 350051, г. Краснодар, ул. Рашпилевская, д. 287, пом. 303

Адрес для почтовой корреспонденции: 350000, г. Краснодар, Бокс №75

Е-mail: support@e-signature.pro

Тел./факс: 8-800-770-01-31

График работы: пн-пт – с 9:00 до 18:00, перерыв с 13:00 до 14:00
сб-вс – выходной



2.3. Порядок информирования о предоставлении услуг УЦ

Информирование по вопросам предоставления услуг Удостоверяющего центра осуществляется следующими способами:

- 1) путем опубликования информации на официальном сайте УЦ: <https://e-signature.pro/>;
- 2) по контактному номеру телефона: 8-800-770-01-31;
- 3) по адресу электронной почты: support@e-signature.pro.

Информирование Удостоверяющим центром заявителей производится посредством направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром, и/или посредством направления SMS-уведомлений на телефонный номер, представленный заявителем в Удостоверяющий центр, и/или посредством размещения информации на официальном сайте УЦ. Выбор способа информирования осуществляется УЦ.

Адреса местонахождения, справочные телефоны и адреса электронной почты доверенных лиц УЦ по приему заявлений на выдачу сертификатов и вручению сертификатов Удостоверяющего центра опубликованы на официальном сайте Удостоверяющего центра.

2.4. Стоимость услуг

Удостоверяющий центр осуществляет свою деятельность на платной основе. Стоимость и состав предоставляемых Удостоверяющим центром услуг устанавливается прайс-листом, размещенном на официальном сайте УЦ. Перечень приобретаемых услуг определяется заявителем из состава услуг УЦ. Сроки и порядок расчетов за оказание услуг Удостоверяющего центра устанавливаются в договорах, заключаемых между УЦ и заявителями, в том числе посредством акцепта Публичной оферты УЦ, размещаемой на официальном сайте УЦ.

Услуги, взимание платы за которые не допускается законодательством РФ, оказываются безвозмездно.

3. Перечень реализуемых удостоверяющим центром функций (оказываемых услуг)

Удостоверяющий центр выполняет следующие функции и оказывает услуги:

- 1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты заявителям при условии идентификации заявителя;
- 2) осуществляет подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному для получения сертификата;
- 3) устанавливает сроки действия сертификатов;
- 4) создает ключи электронной подписи и ключи проверки электронной подписи по обращениям заявителей;
- 5) выдает по обращению заявителя средства электронной подписи, обеспечивающих возможность самостоятельного создания ключа ЭП и ключа проверки ЭП (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- 6) аннулирует сертификаты, выданные Удостоверяющим центром;
- 7) ведет реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных 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;
- 8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- 9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- 10) предоставляет сертификаты ключей проверки электронной подписи в электронной форме, находящихся в реестре созданных сертификатов, по запросам заявителей;



- 11) осуществляет проверку электронных подписей, ключи проверки которых указаны в выданных доверенными лицами УЦ сертификатах ключей проверки электронных подписей;
- 12) обеспечивает электронное взаимодействие доверенных лиц УЦ между собой, а также доверенных лиц с Удостоверяющим центром;
- 13) предоставление сведений об аннулированных сертификатах;
- 14) подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям заявителей;
- 15) подтверждение подлинности электронных подписей уполномоченного лица УЦ в созданных им сертификатах ключей проверки электронной подписи по обращениям заявителей;
- 16) осуществляет иную связанную с использованием электронной подписи деятельность.

4. Права и обязанности Удостоверяющего центра

4.1. Права удостоверяющего центра

Удостоверяющий центр имеет право:

- 1) наделить третьих лиц (далее – доверенное лицо УЦ) на основании заключенного с УЦ соглашения полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра с обязательной идентификацией заявителя при личном присутствии;
- 2) выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе;
- 3) запросить у заявителя документы, подтверждающие указанные в заявлении на выдачу сертификата сведения;
- 4) использовать представленные заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия сертификата, а также иной информации, обязательства по предоставлению которой возложены на УЦ;
- 5) отказать по предусмотренным законами РФ основаниям в создании ключей ЭП и сертификата заявителям, подавшим заявление на их создание, с предоставлением по требованию заявителя письменного мотивированного отказа;
- 6) аннулировать сертификат ключа проверки ЭП в случае установления факта компрометации соответствующего ключа ЭП, с уведомлением владельца данного сертификата ключа проверки ЭП и указанием обоснованных причин;
- 7) раскрыть информацию, относящуюся к конфиденциальной, только в случаях, требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.
- 8) предоставить владельцу сертификата возможность создать электронный образ заявления на выдачу сертификата в целях обеспечения электронного хранения заявительных документов в электронном архиве УЦ.

4.2. Обязанности удостоверяющего центра

Удостоверяющий центр обязан:

- 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;
- 2) обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- 3) предоставлять безвозмездно любому лицу по его обращению информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;
- 4) обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей;
- 5) отказать заявителю в создании сертификата в следующих случаях:



- 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;
 - в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи;
 - в иных случаях, предусмотренных законом.
- 6) хранить в течение всего срока деятельности УЦ информацию, внесенную в реестр сертификатов;
 - 7) внести информацию о сертификате ключа проверки электронной подписи в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата;
 - 8) аннулировать сертификат, если:
 - не подтверждено, что владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП;
 - установлено, что содержащийся в таком сертификате ключ проверки ЭП уже содержится в ином ранее созданном сертификате;
 - вступило в силу решение суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию;
 - по иным основаниям, предусмотренным законом.
 - 9) внести информацию о прекращении действия (аннулировании) сертификата в реестр сертификатов в течение 12 часов с момента, когда УЦ стало известно о наступлении таких обстоятельств;
 - 10) уведомить владельца сертификата об аннулировании, прекращении действия его сертификата посредством публикации списка аннулированных (отозванных) сертификатов;
 - 11) хранить в течение срока деятельности УЦ информацию, указанную в ч. 1 ст. 15 Федерального закона РФ от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», в форме, позволяющей проверить ее целостность и достоверность;
 - 12) использовать для подписания только квалифицированных сертификатов квалифицированную электронную подпись уполномоченного лица УЦ, основанную на квалифицированном сертификате, выданном ему уполномоченным федеральным органом;
 - 13) обеспечить любому лицу безвозмездный доступ к реестру сертификатов УЦ в любое время, за исключением планового и внепланового технического обслуживания, в течение срока деятельности этого УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами;
 - 14) обеспечивать достоверность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
 - 15) в случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр:
 - 1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности УЦ;
 - 2) передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным удостоверяющим центром квалифицированных сертификатов;
 - 3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре. Ключи электронной подписи, хранимые аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи подлежат уничтожению в порядке, установленном федеральным органом исполнительной власти в области обеспечения безопасности.
 - 16) соблюдать положения настоящего Порядка;
 - 17) при выдаче сертификата идентифицировать заявителя – физическое лицо, обратившееся в УЦ за получением сертификата;
 - 18) предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации (далее – ЕСИА) и информации из единой биометрической системы (далее – ЕБС). При этом в случае, если физическое лицо для



- предоставления своих биометрических персональных данных в целях проведения его идентификации в Удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети «Интернет» при выдаче сертификата отказывается от использования шифровальных (криптографических) средств, Удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата;
- 19) осуществить с использованием информационно-технологической и коммуникационной инфраструктуры, определенной Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
 - 20) отказать заявителю в выдаче сертификата в случае, если указанная в п. 5.2.5 настоящего Порядка проверка достоверности документов и сведений не пройдена успешно;
 - 21) при получении квалифицированного сертификата заявителем ознакомить заявителя с информацией, содержащейся в выданном ему сертификате, и хранить такую информацию в течение всего срока осуществления деятельности УЦ;
 - 22) одновременно с выдачей квалифицированного сертификата предоставить владельцу сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
 - 23) направить в ЕСИА сведения о выданном сертификате;
 - 24) осуществить регистрацию владельца сертификата по его желанию в ЕСИА с проведением идентификации владельца при его личном присутствии;
 - 25) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
 - 26) обеспечить конфиденциальность персональной информации о владельце сертификата, за исключением информации, которая непосредственно вносится Удостоверяющим центром в выдаваемый сертификат;
 - 27) выполнять иные обязанности, предусмотренные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» и возложенные на удостоверяющий центр.

4.3. Права заявителя и владельца сертификата

Заявитель и владелец сертификата имеют право:

- 1) обращаться с заявлением на выдачу сертификата в Удостоверяющий центр за получением сертификата, в т. ч. создания ключа ЭП и ключа проверки ЭП;
- 2) обращаться в Удостоверяющий центр за получением средств электронной подписи, обеспечивающих возможность самостоятельного создания ключа ЭП и ключа проверки ЭП;
- 3) обращаться в Удостоверяющий центр с заявлением о прекращении действия сертификата, выданного этим Удостоверяющим центром, при условии, что срок действия соответствующего ключа электронной подписи не истек;
- 4) получать в электронной форме списки аннулированных (отозванных) сертификатов, изготовленные УЦ;
- 5) получать в электронной форме сертификаты уполномоченного лица УЦ;
- 6) получать в электронной форме сертификаты, находящихся в реестре сертификатов ключей проверки ЭП УЦ;
- 7) применять сертификат ключа проверки ЭП уполномоченного лица УЦ для проверки электронной подписи уполномоченного лица УЦ в сертификатах, созданных Удостоверяющим центром;
- 8) применять сертификаты ключа проверки ЭП для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в этих сертификатах;
- 9) применять список аннулированных (отозванных) сертификатов ключей проверки ЭП, созданный Удостоверяющим центром, для проверки их статуса;
- 10) обращаться в УЦ за подтверждением подлинности электронных подписей в электронных документах;
- 11) обратиться в УЦ за подтверждением подлинности электронных подписей уполномоченного лица УЦ в созданных им сертификатах ключей проверки ЭП;



- 12) использовать сервисы службы актуальных статусов сертификатов и службы штампов времени Удостоверяющего центра.
- 13) создать посредством личного кабинета клиента, размещенного на официальном сайте УЦ, электронный образ заявления на выдачу сертификата в целях обеспечения электронного хранения заявительных документов.

4.4. Обязанности владельца сертификата

Владелец сертификата обязан:

- 1) представить в Удостоверяющий центр документы, предусмотренные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем, и иные необходимые для создания сертификата документы;
- 2) обеспечивать конфиденциальность своих ключей электронной подписи, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
- 3) не использовать ключ электронной подписи, сертификат которой выдан УЦ, и немедленно обратиться в УЦ с заявлением о прекращении действия сертификата, при наличии оснований полагать, что конфиденциальность этого ключа электронной подписи нарушена;
- 4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».
- 5) 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.

5. Порядок и сроки выполнения процедур (действий) необходимых для предоставления услуг Удостоверяющим центром

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

5.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей

В соответствии с ч. 4 ст. 5 Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется заявителем самостоятельно на своем автоматизированном рабочем месте в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Удостоверяющий центр осуществляет для заявителя создание ключей электронной подписи и ключей 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 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических)



средств защиты информации (Положение ПКЗ-2005)» на автоматизированном рабочем месте УЦ, которое соответствует требованиям к безопасности при обработке конфиденциальной информации.

5.1.2. Порядок и сроки смены ключей электронной подписи Удостоверяющего центра

Максимальный срок действия ключа ЭП и сертификата ключа проверки ЭП Удостоверяющего центра (уполномоченного лица УЦ) определяется требованиями применяемого в УЦ средства криптографической защиты информации. Основанием для плановой смены ключей Удостоверяющего центра является истечение срока его действия для подписания сертификатов.

Плановая смена ключа ЭП и соответствующего ему ключа проверки ЭП уполномоченного лица УЦ должна выполняться в течение срока действия ключа ЭП уполномоченного лица УЦ.

Процедура плановой смены ключей уполномоченного лица УЦ осуществляется в следующем порядке:

- 1) уполномоченное лицо УЦ формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- 2) уполномоченное лицо УЦ направляет соответствующий запрос на сертификат в головной удостоверяющий центр, функции которого осуществляет уполномоченный федеральный орган;
- 3) после получения сертификата УЦ от головного удостоверяющего центра, новые ключ ЭП и соответствующий ему ключ проверки ЭП уполномоченного лица УЦ используются для подписания сертификатов.

Старый ключ ЭП уполномоченного лица УЦ используется в течение своего срока действия для формирования списков аннулированных (отозванных) сертификатов в электронной форме, созданных Удостоверяющим центром в период действия старого ключа ЭП уполномоченного лица УЦ.

Информирование владельцев сертификатов о плановой смене ключей электронной подписи Удостоверяющего центра осуществляется путем размещения информации на официальном сайте УЦ. Владельцы сертификатов могут получить новый сертификат Удостоверяющего центра из реестра сертификатов уполномоченного федерального органа или путем обращения в Удостоверяющий центр.

5.1.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности

В процессе использования ключей ЭП существуют угрозы нарушения конфиденциальности, которые при использовании уязвимостей информационной системы реализуются в виде атак. К основным категориям атак относятся: отказ в обслуживании, раскрытие информации, нарушение целостности.

Под компрометацией ключа ЭП понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествя, в результате которых ключ ЭП может стать доступным несанкционированным лицам и (или) процессам. К событиям, связанным с компрометацией ключей ЭП относятся, включая, но не ограничиваясь, следующие:

- Потеря носителей, содержащих ключ ЭП.
- Потеря носителей, содержащих ключ ЭП, с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключам ЭП.
- Нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП.
- Возникновение подозрений об утечке информации или ее искажения в системе конфиденциальной связи.
- Нарушение печати на сейфе с носителями, содержащими ключи ЭП.
- Случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключи ЭП (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).



Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа ЭП уполномоченного лица УЦ. Процедура внеплановой смены ключей уполномоченного лица УЦ выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица УЦ. При этом прекращается действие сертификата скомпрометированного ключа ЭП Удостоверяющего центра.

При внеплановой смене ключа ЭП Удостоверяющего центра прекращается действие всех сертификатов, подписанных этим ключом электронной подписи, с занесением сведений об этих сертификатах в реестр сертификатов. Реестр прекративших свое действие сертификатов подписывается скомпрометированным ключом ЭП Удостоверяющего центра.

Информирование владельцев сертификатов о прекращении действия их сертификатов и внеплановой смене ключей электронной подписи Удостоверяющего центра осуществляется путем направления уведомления на указанную в сертификатах электронную почту и размещения информации на официальном сайте УЦ. Владельцы сертификатов могут получить новый сертификат Удостоверяющего центра из реестра сертификатов уполномоченного федерального органа или путем обращения в Удостоверяющий центр.

5.1.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца сертификата

Смена ключа электронной подписи владельца сертификата может осуществляться УЦ в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Смена ключа ЭП сопровождается выдачей Удостоверяющим центром нового сертификата по заявлению на выдачу сертификата в соответствии с п. 5.2 настоящего Порядка и прекращением действия/аннулированием соответствующего сертификата в соответствии с п. 5.4 настоящего Порядка.

5.2. Процедура создания и выдачи Сертификатов

5.2.1. Порядок подачи заявления на создание и выдачу Сертификатов

Заявитель обращается в Удостоверяющий центр или к доверенному лицу УЦ, адреса которых указаны на официальном сайте, с заявлением на выдачу сертификата, оформленного на бумажном носителе.

Заявитель также может подать в Удостоверяющий центр заявление на выдачу сертификата в форме электронного документа, подписанного действующей квалифицированной ЭП, 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 Правительством Российской Федерации, 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" (далее - единая система идентификации и аутентификации) 3 и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных".

5.2.2. Требования к заявлению на создание и выдачу Сертификатов

Форма заявления на выдачу сертификата устанавливается Удостоверяющим центром. Актуальную форму заявления на выдачу сертификата Удостоверяющий центр определяет самостоятельно и



предоставляет по запросу, направленному по адресу электронной почты: support@e-signature.pro. Удостоверяющий центр по своей инициативе вправе вносить в форму заявления любые изменения без уведомления участников электронного взаимодействия.

Заявление на выдачу сертификата может быть оформлено как на бумажном носителе, подписанное заявителем собственноручно, так и в электронном виде, подписанное квалифицированной ЭП заявителя, 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 Правительством Российской Федерации, 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" и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных".

Собственноручное подписание заявления на выдачу сертификата на бумажном носителе производится чернилами (пастой) синего цвета. Использование факсимиле (клише подписи) на заявлении на выдачу сертификата не допускается.

Удостоверяющий центр принимает заявление на выдачу сертификата в электронном виде, подписанное квалифицированной ЭП заявителя, сертификат которой выдан любым удостоверяющим центром, аккредитованным в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», посредством личного кабинета клиента, размещенного на официальном сайте УЦ.

5.2.3. Порядок идентификации заявителя

Идентификация заявителя – физического лица проводится при его личном присутствии по основному документу, удостоверяющему личность, 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 Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом 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.

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.



5.2.4. Перечень документов для создания и выдачи Сертификатов

При обращении в Удостоверяющий центр заявитель предоставляет заявление на выдачу сертификата и документы либо их надлежащим образом заверенные копии и (или) сведения из них, необходимые для удостоверения заявителя – физического лица, а также документы, на основании которых Удостоверяющим центром вносятся сведения в сертификат, такие как:

- 1) основной документ, удостоверяющий личность;
- 2) страховой номер индивидуального лицевого счета заявителя – физического лица;
- 3) идентификационный номер налогоплательщика заявителя – физического лица;

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

Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органами власти.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

Удостоверяющий центр выполняет свою обязанность по внесению в сертификат только достоверной и актуальной информации путем сбора и хранения скан-копий документов, представленных заявителем, а также путем запроса соответствующих сведений из информационных систем органов государственной власти.

5.2.5. Порядок проверки достоверности документов и сведений, предоставленных заявителем

Для заполнения сертификата в соответствии с частью 2 статьи 17 Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в сертификат, и Удостоверяющим центром идентифицирован заявитель – физическое лицо, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю сертификата. В противном случае Удостоверяющий центр отказывает заявителю в выдаче сертификата.

5.2.6. Порядок создания Сертификата

Сертификат создается Удостоверяющим центром с помощью сертифицированных средств удостоверяющего центра на основании заявления на выдачу сертификата и, в случае предоставления заявителем, запроса на сертификат в формате, описанном в рекомендациях IETF RFC 2986 PKCS #10: Certification Request Syntax Specification.

Удостоверяющий центр издает сертификаты в форме электронного документа формата X.509 версии 3.

Удостоверяющий центр по основаниям, предусмотренным действующим законодательством, вправе отказать в создании сертификата.



5.2.7. Порядок выдачи Сертификата

Выдача сертификата Удостоверяющим центром осуществляется после успешной идентификации заявителя в соответствии с п. 5.2.3 настоящего Порядка. При выдаче сертификата, его владельцу выдается ключ ЭП и ключ проверки ЭП, в случае их создания Удостоверяющим центром, а также предоставляется руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При получении квалифицированного сертификата заявителем удостоверяющий центр ознакомливает его с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

При выдаче сертификата Удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. По желанию лица, которому выдан квалифицированный сертификат, Удостоверяющий центр осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

5.2.8. Сроки создания и выдачи Сертификата

Срок создания и выдачи сертификата с момента получения Удостоверяющим центром соответствующего заявления составляет не более 5 календарных дней, при условии подтверждения соответствия сведений в заявлении на выдачу.

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

Подтверждение действительности ЭП в электронном документе осуществляется на основании заявления на подтверждение действительности ЭП, форма которого установлена Приложением № 1 к настоящему Порядку. Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является носитель, содержащий следующие файлы:

- 1) файл, содержащий электронный документ, к которому применена электронная подпись;
- 2) файл, содержащий электронную подпись формата PKCS#7 электронного документа, к которому применена электронная подпись;
- 3) файл, содержащий сертификат электронного документа вместе с цепочкой сертификатов издателей;
- 4) файл, содержащий список аннулированных (отозванных) сертификатов УЦ, являющегося издателем сертификата электронного документа, и использовавшийся для проверки ЭП электронного документа заявителем.

Срок проведения работ по подтверждению действительности ЭП в электронном документе составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр и при наличии оплаты стоимости данных услуг согласно прайс-листу УЦ.



Процедура подтверждения действительности ЭП осуществляется с использованием программного комплекса, входящего в состав сертифицированного программно-аппаратного комплекса Удостоверяющего центра, комиссией, сформированной из числа сотрудников УЦ.

Проверка действительности ЭП включает в себя:

- 1) определение сертификата или нескольких сертификатов, необходимых для проверки ЭП;
- 2) проверку ЭП электронного документа с использованием каждого сертификата;
- 3) определение даты формирования каждой ЭП в электронном документе;
- 4) проверку ЭП каждого сертификата, путем построения цепочки сертификатов до сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром;
- 5) проверку действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром на текущий момент времени, путем проверки отсутствия этих сертификатов в списках отозванных сертификатов (CRL).

По результатам оказания услуги оформляется заключение, содержащее информацию действительности ЭП, использованной для подписания электронного документа.

Проверка ЭП под электронными документами осуществляется только при технической совместимости используемых средств Удостоверяющего центра. При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

5.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата

5.4.1. Основания прекращения действия или аннулирования Сертификата

Сертификат прекращает свое действие в случаях, установленных Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

- 1) не подтверждено, что владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;
- 2) установлено, что содержащийся в сертификате ключ проверки ЭП уже содержится в ином ранее созданном сертификате;
- 3) вступило в силу решение суда, которым установлено, что сертификат содержит недостоверную информацию.
- 4) иных случаях, предусмотренных действующим законодательством.

5.4.2. Порядок действий Удостоверяющего центра при прекращении действия сертификата

Заявление о прекращении действия сертификата ключа проверки ЭП подается в УЦ в бумажной форме при личном прибытии владельца сертификата в УЦ (доверенному лицу УЦ) или форме электронного документа, подписанного усиленной квалифицированной ЭП владельца сертификата, в том числе с использованием федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)".

Прекращение действия сертификата ключа проверки ЭП, созданного Удостоверяющим центром, осуществляется Удостоверяющим центром по заявлению о прекращении действия сертификата. Форма заявления о прекращении действия сертификата устанавливается Удостоверяющим центром и предусматривает указание в заявлении серийного номера квалифицированного сертификата, даты начала и окончания действия квалифицированного сертификата, наименования Удостоверяющего центра, выдавшего квалифицированный сертификат, причины прекращения действия квалифицированного сертификата, а также, в отношении физического лица: фамилии, имени, отчества (при наличии), страхового номера индивидуального лицевого счета, идентификационного номера налогоплательщика. Актуальную



форму заявления о прекращении действия сертификата Удостоверяющий центр предоставляет по запросу, направленному по адресу электронной почты: support@e-signature.pro. Удостоверяющий центр по своей инициативе вправе вносить в форму заявления о прекращении действия любые изменения без уведомления участников электронного взаимодействия.

В случае направления заявителем заявления о прекращении действия квалифицированного сертификата с использованием федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)" принятое по такому заявлению решение Удостоверяющего центра в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Удостоверяющего центра, размещается в личном кабинете заявителя в системе "Единый портал государственных и муниципальных услуг (функций)" после проведения проверки действительности усиленной квалифицированной электронной подписи Удостоверяющего центра, которой такое решение подписано, и подтверждения ее действительности. В случае принятия по такому заявлению решения об аннулировании квалифицированного сертификата Удостоверяющий центр после внесения соответствующей информации в реестр квалифицированных сертификатов направляет в систему "Единый портал государственных и муниципальных услуг (функций)" информацию об аннулировании квалифицированного сертификата.

Приём заявлений о прекращении действия сертификата в бумажной форме осуществляется в рабочие дни УЦ с 09:00 до 18:00.

Информация о прекращении действия или аннулировании сертификата вносится в реестр сертификатов в срок не более 12 (двенадцати) часов с момента приема заявления о прекращении действия сертификата или наступления иного события, предусмотренного подразделом 5.4.1 настоящего Порядка. Действие сертификата прекращается с момента публикации реестра сертификатов, в который внесён данный сертификат.

Адреса публикации реестра аннулированных (отозванных) сертификатов заносятся в созданные Удостоверяющим Центром сертификаты в расширение CRL Distribution Point сертификата.

5.5. Порядок ведения реестра Сертификатов

Хранение информации, содержащейся в реестре сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Хранение в Удостоверяющем центре всех выданных сертификатов осуществляется постоянно в форме электронных документов. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Срок внесения в реестр сертификатов сведений о прекращении действия или аннулировании сертификатов составляет не более 12 (двенадцати) часов с момента приема заявления о прекращении действия сертификата или наступления иного события, предусмотренного подразделом 5.4.1 настоящего Порядка.

Удостоверяющий центр обеспечивает доступность реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра сертификатов.



5.6. Порядок технического обслуживания Реестра сертификатов

Срок планового технического обслуживания реестра сертификатов составляет не более 4 (четырёх) часов. В случае необходимости может проводиться внеплановое техническое обслуживание программно-аппаратных и технических средств УЦ и реестра сертификатов, срок которого составляет не более 4 (четырёх) часов. Срок проведения внепланового технического обслуживания может быть увеличен по объективным причинам. Удостоверяющий центр информирует о проведении технического обслуживания посредством размещения информации на официальном сайте Удостоверяющего центра.

6. Порядок исполнения обязанностей удостоверяющего центра

6.1. 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

Удостоверяющий центр информирует заявителя об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки, путем предоставления Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, которое размещено на официальном сайте УЦ.

6.2. Обеспечение актуальности информации, содержащейся в Реестре сертификатов, и ее защиты

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов, путем соблюдения сроков внесения сведений о прекращении действия и/или аннулировании сертификатов, установленных Федеральным законом № 63-ФЗ.

Защита информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем:

- предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременным обнаружением фактов несанкционированного доступа к информации;
- недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможностью восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- контролем за обеспечением уровня защищенности информации;
- нахождением баз данных информации в контролируемой зоне, исключая свободное пребывание посторонних лиц;
- использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

6.3. Обеспечение доступности Реестра сертификатов

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к Реестру сертификатов, через форму запроса на официальном сайте Удостоверяющего центра, в любое время, за исключением периодов технического обслуживания Реестра сертификатов.

Доступ к Реестру сертификатов осуществляется через форму запроса, размещенной по адресу <https://e-signature.pro/registry>



6.4. Обеспечение конфиденциальности созданных УЦ ключей электронных подписей

Обеспечение конфиденциальности созданных Удостоверяющим центром ключей электронных подписей достигается путем создания их на автоматизированном рабочем месте УЦ, которое соответствует требованиям к безопасности при обработке конфиденциальной информации.

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

При выдаче сертификата Удостоверяющий центр направляет в Единую систему идентификации и аутентификации (далее – ЕСИА) сведения о владельце сертификата, в объеме, необходимом для регистрации в ЕСИА, и о полученном им сертификате (уникальный номер сертификата, даты начала и окончания его действия, наименование Удостоверяющего центра).

При выдаче сертификата Удостоверяющий центр по желанию лица, которому выдан сертификат, безвозмездно осуществляет регистрацию владельца сертификата в ЕСИА.

7. Дополнительные положения

7.1. Подтверждение владения ключом ЭП, соответствующим сертификату ключа проверки ЭП

Подтверждение владения заявителем ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения сертификата, осуществляется в соответствии с правилами подтверждения владения ключом электронной подписи, утвержденными приказом ФСБ России от 20.04.2021 г. № 154, за исключением, когда ключ ЭП и ключ проверки ЭП создаются УЦ для заявителя.

В случае создания ключа ЭП и ключа проверки ЭП для заявителя Удостоверяющим центром, владение заявителем ключом ЭП подтверждается распиской об ознакомлении с информацией, содержащейся в выдаваемом квалифицированном сертификате.

7.2. Предоставление сервисов Службы актуальных статусов сертификатов и Службы штампов времени

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов.

Служба актуальных статусов сертификатов по запросам владельцев сертификатов формирует и предоставляет OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата.

OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата Службы актуальных статусов сертификатов Удостоверяющего центра. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- 1) выполнены условия признания квалифицированной электронной подписи в OCSP-ответе;
- 2) квалифицированная электронная подпись в OCSP-ответе сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы актуальных статусов сертификатов, а именно: сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.9 – «Подпись ответа службы OCSP».

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центром сертификатов ключей проверки электронной подписи.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному электронной подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

- выполнены условия признания квалифицированной электронной подписи в штампе времени;



- квалифицированная электронная подпись в штампе времени сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы штампов времени, а именно: сертификат ключа проверки электронной подписи Службы штампов времени в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.8 – «Установка штампа времени».

Адрес обращения к Службе штампов времени Удостоверяющего центра предоставляется по запросу, направленному по адресу электронной почты: support@e-signature.pro.



ЗАЯВЛЕНИЕ НА ПОДТВЕРЖДЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ В ЭЛЕКТРОННОМ ДОКУМЕНТЕ

Для физических лиц

Я, _____

(фамилия, имя, отчество)

Прошу подтвердить действительность электронной подписи в документе

(указать наименование документа)

на основании следующих данных:

- 1) Файл, содержащий электронный документ, к которому применена электронная подпись;
- 2) Файл, содержащий электронную подпись формата PKCS#7 электронного документа, к которому применена электронная подпись;
- 3) Файл, содержащий сертификат, с использованием которого необходимо осуществить проверку электронной подписи в электронном документе, вместе с цепочкой сертификатов издателей;
- 4) Файл, содержащий список аннулированных (отозванных) сертификатов УЦ, являющегося издателем сертификата электронного документа, и использовавшийся для проверки ЭП электронного документа заявителем.
- 5) Время¹ подписания электронной подписью электронного документа:

« _____ : _____ » « _____ / _____ / _____ »;

Час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

« _____ : _____ » « _____ / _____ / _____ »;

Час минута день месяц год

Приложение: носитель, содержащий указанные выше файлы.

(подпись)

(фамилия, инициалы)

« _____ » _____ 20 ____ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Москвы