Основание
Удостоверяющий центр

УТВЕРЖДАЮ
Генеральный директор
АО «Аналитический Центр»

_____С.Ю. Белоногов

30 октября 2024 года

РЕГЛАМЕНТ

порядок реализации функций удостоверяющего центра АО «Аналитический Центр» и исполнения его обязанностей

Содержание

Термины и определения 4
1. Общие положения 6
1.1. Предмет регулирования 6
1.2. Сведения об Удостоверяющем центре 7
1.3. Порядок информирования о предоставлении услуг Удостоверяющего центра 8
1.4. Стоимость услуг Удостоверяющего центра 8
2. Функции (оказываемые услуги) Удостоверяющего центра 10
2.1. Назначение Удостоверяющего центра 10
2.2. Функции (оказываемые услуги) Удостоверяющего центра: 10
3. Права и обязанности Сторон Регламента 12
3.1. Права и обязанности Удостоверяющего центра: 12
3.2. Права и обязанности заявителя 16
3.3. Права и обязанности Пользователей 17
4. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющего центра 20
4.1. Процедура создания ключей ЭП и ключей проверки ЭП 20
4.2. Процедура создания и выдачи Сертификатов 23
4.3. Подтверждение действительности ЭП, использованной для подписания электронных документов 28
4.4. Процедуры, осуществляемые при прекращении действия (аннулировании) Сертификата 29
4.5. Ведение Реестра сертификатов 32
4.6. Порядок технического обслуживания Реестра сертификатов 33
5. Порядок исполнения обязанностей Удостоверяющего центра 34
5.1. Информирование заявителей об условиях и о порядке использования электронной подписи и средств электронной подписи, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки 34
5.2. Выдача по обращению заявителя (Пользователя) средств электронной подписи 34
5.3. Обеспечение актуальности информации, содержащейся в Реестре сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий 34
5.4. Обеспечение доступности Реестра сертификатов 35

5.5. Порядок обеспечения конфиденциальности созданных УЦ ключей ЭП. 35
5.6. Осуществление регистрации Сертификата и лица, которому выдан Сертификат, в единой системе идентификации и аутентификации 36
5.7. Предоставление доступа к информации, содержащейся в Реестре сертификатов. 36
6. Иные положения..... 37
6.1. Конфиденциальность информации 37
6.2. Хранение информации в Удостоверяющем центре..... 37
6.3. Ответственность сторон Регламента..... 38
6.4. Разрешение споров..... 38
7. Список приложений 39
Приложение №1: Форма заявления на создание и выдачу Сертификата……..……40
Приложение №2: Форма заявления на прекращение действия Сертификата..41
Приложение №3: Форма заявления на подтверждение действительности электронной подписи в электронном документе……42
Приложение №4: Форма заявления на смену ключа электронной подписи…43
Приложение №5: Перечень документов, представляемых для создания и выдачи Сертификата……..44
Приложение №6: Форма Акта отказа от фотофиксации……...45
Приложение№7: Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи……46
Приложение №8: Структура СОС УЦ……..…48

Термины и определения

Для целей настоящего Порядка реализации функций удостоверяющего центра АО «Аналитический Центр» и исполнения его обязанностей (Регламент) (далее – Регламент) используются термины и их определения, установленные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – ФЗ «Об электронной подписи»), а также дополнительно к ним в специальном значении используются следующие термины и их определения:

Удостоверяющий центр (УЦ) – АО «Аналитический Центр», выполняющее функции аккредитованного удостоверяющего центра в соответствии с ФЗ «Об электронной подписи».

Доверенное лицо УЦ – представитель УЦ, на основании соглашения осуществляющий прием заявлений на создание и выдачу Сертификатов, заявлений на досрочное прекращение действия Сертификатов, личную идентификацию заявителя, а также вручение Сертификатов от имени УЦ.

ЭП – электронная подпись.

Компрометация ключа ЭП – нарушение или обоснованное подозрение в нарушении конфиденциальности ключа ЭП, в том числе хищение, утрата, разглашение ключа ЭП и другие случаи, в результате которых ключ ЭП мог стать доступными несанкционированным лицам и (или) процессам.

Ключевая информация – ключ ЭП и ключ проверки ЭП.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Заявитель – физическое лицо, обратившееся в Удостоверяющий центр за получением Сертификата в качестве его будущего владельца.

Пользователь – Заявитель, присоединившийся к Регламенту, сведения о котором внесены в Реестр, а также юридическое лицо, которому до 01.09.2023 выдан Сертификат с указанием в нем наряду с этим юридическим лицом также его работника, действующего от его имени по доверенности, в лице своего уполномоченного представителя.

Реестр – набор документов УЦ, включающий реестр Пользователей, реестр выданных и аннулированных УЦ Сертификатов (далее — Реестр сертификатов), Список отозванных сертификатов УЦ.

Сертификат – квалифицированный сертификат ключа проверки электронной подписи. УЦ не осуществляет создание и выдачу неквалифицированных сертификатов ключей проверки ЭП.

Список отозванных сертификатов (СОС) – электронный документ с ЭП, включающий в себя список серийных номеров Сертификатов, которые на определенный момент были аннулированы или действие которых было досрочно прекращено.

Уполномоченный федеральный орган – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Усиленная квалифицированная электронная подпись (УКЭП) – ЭП, полученная в результате криптографического преобразования информации с использованием ключа ЭП и средств (средства) ЭП, имеющих (имеющего) подтверждение соответствия требованиям, установленным в соответствии с ФЗ «Об электронной подписи», позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания, ключ ЭП которой указан в Сертификате.

1. Общие положения

1.1. Предмет регулирования

1.1.1. Настоящий Регламент определяет условия предоставления услуг УЦ, включая права, обязанности, ответственность УЦ, Заявителей и Пользователей, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы УЦ.

1.1.2. Регламент является договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации. Все приложения, изменения и дополнения к нему являются его неотъемлемой частью.

1.1.3. Регламент размещен в электронной форме по адресу: https://uc-osnovanie.ru/docs/UC-Osnovanie-reglament-AO-AC.pdf

1.1.4. Фактом присоединения к Регламенту является прием УЦ от Заявителя Заявления на создание и выдачу Сертификата.

1.1.5. Факт присоединения Заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений.

УЦ и лицо, присоединившиеся к Регламенту, вступают в соответствующие договорные отношения на срок действия Сертификата, полученного им в УЦ.

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

1.1.7. Актуальная редакция Регламента размещается на сайте УЦ в информационно-телекоммуникационной сети «Интернет» по адресу: https://uc-osnovanie.ru/ (далее – сайт УЦ).

1.1.8. Все изменения (дополнения), вносимые УЦ в Регламент и не связанные с изменением действующего законодательства, вступают в силу и становятся обязательными по истечении 10 (десяти) календарных дней с даты размещения новой редакции Регламента на сайте УЦ.

Все изменения (дополнения), вносимые УЦ в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений в действующем законодательстве.

1.1.9. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

1.1.10. В случае несогласия с изменениями (дополнениями) Регламента Пользователь имеет право до вступления в силу таких изменений (дополнений) прекратить взаимодействие с УЦ в рамках Регламента, обратившись в УЦ с Заявлением на прекращение действия имеющихся у него Сертификатов. При этом вознаграждение УЦ за выдачу указанных Сертификатов не возвращается.

Отсутствие указанного в настоящем пункте заявления Пользователя расценивается УЦ как акцепт новой редакции и изменений Регламента в соответствии с п. 2 ст. 438 Гражданского кодекса Российской Федерации.

1.2. Сведения об Удостоверяющем центре

1.2.1 Общие сведения

Полное наименование: Акционерное общество «Аналитический Центр»

Сокращенное наименование: АО «Аналитический Центр»

Коммерческое обозначение: Удостоверяющий центр «Основание»

Основной государственный регистрационный номер: 1105260001175

ИНН/КПП: 5260270696/770901001

Юридический адрес: 105005, город Москва, улица Радио, дом 24, корпус 2, помещение 1П/6.

Адрес для почтовых отправлений: 603000, г. Нижний Новгород, ул. Ульянова, д. 10а, пом. П52а, ком. 501 (обособленное подразделение АО «Аналитический Центр» в г. Нижний Новгород).

Контактный (справочный) телефон: 8-800-101-41-40

Адреса мест нахождения обособленных подразделений (филиалов) УЦ указаны на сайте УЦ.

1.2.2. Удостоверяющий центр осуществляет деятельность по созданию и выдачи Сертификатов на основании следующих документов:

– Лицензия ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых 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: регистрационный номер Л051-00105-00/00145929 (18148 Н) от 25.11.2020;

– Решение Правительственной комиссии, уполномоченной на принятие решений об аккредитации удостоверяющих центров (протокол от 04.12.2023 №10пр).

1.2.3. График работы УЦ и его обособленных подразделений: с 9.00 по 18.00 (время по месту нахождения подразделения УЦ, в котором осуществляется обслуживание) каждого дня недели, за исключением выходных и праздничных дней.

График работы информационно-справочной поддержки: круглосуточно.

1.3. Порядок информирования о предоставлении услуг Удостоверяющего центра

1.3.1. Информация по вопросам предоставления услуг УЦ может быть получена на сайте УЦ, по телефону, посредством направления электронного письма на адрес электронной почты УЦ, через сервис обмена сообщениями на сайте УЦ, телеграм бот или при личном обращении заинтересованных лиц в УЦ и его обособленные подразделения (филиалы).

Справочный телефон УЦ: 8-800-101-41-40

Адрес электронной почты УЦ: info@uc-osnovanie.ru

Адрес электронной почты УЦ по вопросам технической поддержки: help@uc-osnovanie.ru

Сайт УЦ в информационно-телекоммуникационной сети «Интернет»: https://uc-osnovanie.ru/

Телеграм бот: @Tech_AC_bot

Справочные телефоны и адреса электронной почты обособленных подразделений (филиалов) УЦ опубликованы на сайте УЦ по адресу: https://uc-osnovanie.ru/contacts.html

1.3.2. В случае изменения контактных (справочных) телефонов и (или) адресов электронной почты информация об актуальных телефонах и адресах электронной почты размещается на сайте УЦ.

1.3.3. УЦ обеспечивает круглосуточный прием запросов на электронную почту. Прием звонков по справочному телефону УЦ осуществляется круглосуточно.

1.3.4. Ответ на обращение, поступившее на электронную почту УЦ, направляется на адрес электронной почты, с которого поступило обращение, или указанному в обращении в качестве адреса направления ответа адресу электронной почты. При этом УЦ не несет ответственности за неполучение отправленного по указанным адресам ответа.

1.4. Стоимость услуг Удостоверяющего центра

1.4.1. УЦ осуществляет свою деятельность на платной основе.

1.4.2. Размер установленной УЦ платы за создание и выдачу Сертификата не может превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

1.4.3. Оплата услуг УЦ осуществляется путем 100% (стопроцентной) предоплаты в российских рублях по безналичной форме в течение 5 (пяти) банковских дней с момента выставления счета УЦ на расчетный счет УЦ, указанный в выставленном УЦ счете.

1.4.4. Датой оплаты услуг, оказываемых УЦ, считается дата зачисления денежных средств на расчетный счет УЦ, указанный в счете.

1.4.5. Информация о стоимости услуг УЦ размещается на сайте УЦ, предоставляется по справочному телефону, на адрес электронной почты, а также при личной явке в УЦ или его обособленное подразделение (филиал).

1.4.6. Пользователь обязан принять оказанные УЦ услуги, подписав в качестве акта об оказанных услугах Универсальный передаточный документ (далее – УПД) по форме, рекомендованной Федеральной налоговой службой (письма ФНС России от 21.10.2013 № ММВ-20-3/96@ и от 17.10.2014 №ММВ-20-15/86@).

В случае непоступления от Пользователя подписанного УПД либо мотивированных замечаний к нему в течение 3 (трёх) дней с момента его получения, услуги УЦ считаются оказанными надлежащим образом и принятыми Пользователем без замечаний.

1.4.7. Особенности оплаты и оказания услуг УЦ могут устанавливаться договорами с УЦ.

2. Функции (оказываемые услуги) Удостоверяющего центра

2.1. Назначение Удостоверяющего центра

2.1.1. УЦ предназначен для оказания услуг по созданию, выдаче и прекращению действия (аннулированию) Сертификатов, а также для предоставления иных услуг, определенных ФЗ «Об электронной подписи».

2.1.2. Созданные УЦ Сертификаты могут использоваться для:

- применения ЭП;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе обмена электронными документами;
- аутентификации участников информационного взаимодействия в процессе обмена электронными документами;
- обеспечения конфиденциальности информации, представленной в электронном виде.

2.2. Функции (оказываемые услуги) Удостоверяющего центра:

- создание и выдача Сертификатов по обращениям Заявителей и Пользователей-физических лиц при условии идентификации заявителя (Пользователя УЦ-физического лица) в соответствии с требованиями статьи 18 ФЗ «Об электронной подписи»;
- осуществление в соответствии с правилами подтверждения владения ключом ЭП подтверждения владения Заявителем (Пользователем-физическим лицом) ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения Сертификата;
- создание и выдача сертификатов ключей проверки ЭП заявителям в отношении усиленной неквалифицированной ЭП, что может осуществляться при определении лица, подающего заявление в электронной форме без личного присутствия способами, предусмотренными пунктами 1 и 1.2. части 1 статьи 13 ФЗ «Об электронной подписи» (в случае начала осуществления УЦ деятельности по созданию и выдаче неквалифицированных сертификатов ключей проверки ЭП);
- установление сроков действия Сертификатов;
- прекращение действия (аннулирование) Сертификатов;
- выдача по обращениям заявителей (Пользователей) средств ЭП, содержащих ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП;
- ведение Реестра сертификатов;
- установление порядка ведения реестра сертификатов, не являющихся квалифицированными, и порядка доступа к нему (в случае начала осуществления УЦ деятельности по созданию и выдаче

неквалифицированных сертификатов ключей проверки ЭП), а также обеспечение доступа к информации, содержащейся в Реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

- создание для Заявителей и Пользователей –физических лиц ключей ЭП и ключей проверки ЭП;
- проверка уникальности ключей проверки ЭП в Реестре сертификатов;
- осуществление по обращениям проверки ЭП;
- осуществление иной связанной с использованием ЭП деятельности.

3. Права и обязанности Сторон Регламента

3.1. Права и обязанности Удостоверяющего центра:

3.1.1. УЦ имеет право:

− запрашивать у Заявителя (Пользователя) документы и сведения, необходимые для оказания услуг УЦ;

− принимать меры, направленные на обеспечение подтверждения обращения за получением услуг УЦ конкретным лицом, осуществлять фотофиксацию соответствующего факта;

− не принимать от Заявителей (Пользователей) документы, не соответствующие требованиям законодательства Российской Федерации;

− запрашивать в порядке, установленном ФЗ «Об электронной подписи», в государственных информационных системах сведения, необходимые для осуществления проверки документов и сведений, представленных в УЦ для создания Сертификата;

− отказать Заявителю (Пользователю) в создании и выдаче Сертификата в случаях, предусмотренных ФЗ «Об электронной подписи» и Регламентом;

− выдавать Сертификаты как в форме электронных документов, так и по запросу Заявителя в форме документов на бумажном носителе;

− отказать в прекращении действия Сертификата в случае ненадлежащего оформления заявления на прекращения действия Сертификата, неподтверждения полномочий на подачу этого заявления, недействительности квалифицированной электронной подписи, которой подписано указанное заявление в электронной форме, а также если Сертификат уже аннулирован или прекратил свое действие по другим основаниям;

− отказать в выдаче Сертификата в случае, если Заявитель не дал согласие на обработку УЦ его персональных данных, необходимых для создания Сертификата и обслуживания в УЦ;

− досрочно прекратить действие Сертификата в случаях, предусмотренных абзацем 2 пп. 4.4.1 Регламента;

− отказать в предоставлении сведений, содержащихся в Реестре сертификатов, в случае, если объем запрашиваемых данных не соответствует законной цели обработки этих данных, заявленной в запросе на предоставление сведений;

− использовать представленные Пользователем номера мобильной связи и адреса электронной почты для рассылки уведомлений о досрочном прекращении действия Сертификата, окончании срока его действия и иной информации, связанной с реализацией функций УЦ;

− привлекать для приема Заявлений на создание и выдачу Сертификата Заявителей (Пользователей-физических лиц), а также вручения Сертификатов от имени УЦ Доверенных лиц УЦ;

– осуществлять иные права, предусмотренные действующим законодательством и Регламентом.

3.1.2. УЦ обязан:

– выполнять порядок реализации функций аккредитованного УЦ и исполнения его обязанностей, установленный УЦ в соответствии с утвержденными уполномоченным федеральным органом Требованиями к порядку реализации функций аккредитованного УЦ и исполнения обязанностей, а также с ФЗ «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с ФЗ «Об электронной подписи»;

– информировать Заявителей (Пользователей) об условиях и порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки;

– при выдаче Сертификата:

1) Идентифицировать Заявителя (Пользователя – физическое лицо), обратившееся к нему за получением Сертификата;

2) Заявителям (Пользователям-физическим лицам), обратившимся в УЦ в целях проведения идентификации без их личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных Заявителей (Пользователей-физических лиц) в целях проведения их идентификации в УЦ без их личного присутствия посредством сети "Интернет") 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", и указать страницу сайта в сети "Интернет", с которой предоставляются эти средства;

– осуществлять проверку достоверности документов и сведений, представленных Заявителем (Пользователем) для получения Сертификата, с использованием информации из государственных информационных ресурсов;

– отказать в создании Сертификата в следующих случаях:

а) если не удалось идентифицировать Заявителя (Пользователя – физическое лицо);

б) непредставления заявления на создание Сертификата, а также документов и сведений, необходимых в соответствии с действующим законодательством для создания Сертификата, либо представления ненадлежащим образом оформленных указанных документов;

в) неподтверждения того, что Заявитель (Пользователь-физическое лицо) владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному для получения Сертификата;

г) отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки ЭП, указанного для получения Сертификата;

д) неподтверждения достоверности представленных Заявителем (Пользователем-физическим лицом) документов и сведений для включения в Сертификат в ходе их проверки с использованием инфраструктуры, предусмотренной ч. 2.2 ст. 18 ФЗ «Об электронной подписи»;

е) в случае отказа Заявителя (Пользователя-физического лица) от использования шифровальных (криптографических) средств в случае, указанном в п. 4 ч. 1 ст. 18 ФЗ «Об электронной подписи»;

ж) в иных случаях, предусмотренных действующим законодательством.

– при вручении Сертификата ознакомить с информацией, содержащейся в Сертификате, в порядке, предусмотренном ч. 3 ст. 18 ФЗ «Об электронной подписи»;

– хранить информацию, подтверждающую ознакомление заявителя (Пользователя) с информацией, содержащейся в Сертификате, в течение всего срока осуществления своей деятельности;

– предоставить владельцу Сертификата Сертификат УЦ в электронной форме;

– по требованию владельца Сертификата, выданного в форме электронного документа, выдать ему копию Сертификата на бумажном носителе, заверенную УЦ;

– предоставить владельцу Сертификата Руководство по обеспечению безопасности использования квалифицированной ЭП и средств квалифицированной ЭП, размещенное на сайте УЦ;

– использовать для изготовления ключей ЭП и формирования ЭП только средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с ФЗ «Об электронной подписи»;

– создавать Сертификаты с использованием средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленных федеральным органом исполнительной власти в области обеспечения безопасности;

– использовать квалифицированную ЭП, основанную на Сертификате, выданном ему головным УЦ, функции которого осуществляет уполномоченный федеральный орган для подписания от своего имени Сертификатов. УЦ запрещается использовать квалифицированную ЭП, основанную на Сертификате, выданном ему головным УЦ, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами;

– принять меры по защите ключа ЭП УЦ от несанкционированного доступа;

– обеспечить уникальность регистрационной информации Пользователей в Реестре УЦ;

– обеспечить изготовление ключей ЭП и Сертификатов в соответствии с требованиями действующего законодательства и Регламента;

– обеспечить уникальность серийных номеров изготавливаемых Сертификатов, а также значений ключей проверки ЭП в изготовленных Сертификатах;

– обеспечивать конфиденциальность созданных УЦ ключей ЭП;

– прекратить действие Сертификата в случаях, предусмотренных ФЗ «Об электронной подписи» и (или) Регламентом;

– аннулировать Сертификат в случаях, предусмотренных ч. 6.1 ст. 14 ФЗ «Об электронной подписи»;

– до внесения в Реестр сертификатов информации об аннулировании Сертификата уведомить об аннулировании Сертификата владельца Сертификата путем направления электронного документа на представленный им адрес электронной почты или посредством информационной системы УЦ, в которой владелец Сертификата имеет личный кабинет;

– формировать и вести Реестр сертификатов в соответствии с требованиями ФЗ «Об электронной подписи», принимаемых в соответствии с ним нормативных правовых актов и Регламента;

– внести информацию о созданном УЦ Сертификате в Реестр сертификатов не позднее указанной в нем даты начала действия Сертификата;

– внести информацию о прекращении действия (аннулировании) Сертификата в Реестр сертификатов в течение 12 часов с момента наступления обстоятельств, указанных в пп.пп. 4.4.1, 4.4.2 Регламента в качестве оснований для прекращения действия или аннулирования Сертификата, или в течение 12 часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств;

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

– хранить в течение всего срока своей деятельности информацию, внесенную в Реестр сертификатов;

– обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационной сети «Интернет» к Реестру сертификатов в любое время, за исключением периодов планового и внепланового технического обслуживания;

– предоставлять безвозмездно любому лицу по его обращению сведения, содержащиеся в Реестре сертификатов, в том числе информацию о прекращении действия (аннулировании) Сертификата;

– публиковать актуальный СОС как минимум на двух сетевых ресурсах в информационно-телекоммуникационной сети «Интернет», в том числе на сайте УЦ. Адреса распространения СОС заносятся в изготавливаемые УЦ Сертификаты;

– обеспечить в течение всего срока своей деятельности, если иной срок не предусмотрен нормативными правовыми актами Российской Федерации, хранение в электронном виде информации, предусмотренной ч. 1 ст. 15 ФЗ «Об электронной подписи», а именно:

1) реквизиты основного документа, удостоверяющего личность владельца Сертификата – физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени юридического лица, обращаться за получением Сертификата, выданного УЦ до 01.09.2023;

3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца Сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца Сертификата включена в Сертификат;

− предоставить Заявителю (Пользователю) необходимые средства ЭП и права на их использование в соответствии с отдельными договорами;

− в соответствии с ч. 5 ст. 18 ФЗ «Об электронной подписи» направлять в единую систему идентификации и аутентификации сведения о лице, получившем Сертификат, в объеме, необходимом для регистрации в единой информационной системе идентификации и аутентификации, и о полученном им Сертификате;

− по желанию лица, которому выдан Сертификат, безвозмездно осуществлять регистрацию указанного лица в единой системе идентификации и аутентификации;

− в случае принятия решения о прекращении своей деятельности сообщить об этом в уполномоченный федеральный орган и владельцам Сертификатов, которые выданы УЦ и срок действия которых не истек, не позднее чем за один месяц до даты прекращения своей деятельности, а также передать в уполномоченный федеральный орган в установленном порядке Реестр сертификатов и информацию, подлежащую хранению в аккредитованном УЦ;

− нести иные обязанности, предусмотренные ФЗ «Об электронной подписи», принятыми в соответствии с ним нормативными правовыми актами и Регламентом.

3.2. Права и обязанности заявителя

3.2.1. Заявитель вправе:

− получить сведения об УЦ и (или) Доверенном лице УЦ;

− получить информацию о перечне, стоимости, сроках и порядке оказания услуг УЦ;

− ознакомиться с актуальной редакцией Регламента и договоров об оказании услуг УЦ;

− осуществлять иные права, предусмотренные для заявителей, действующим законодательством и Регламентом.

− отказаться от фотофиксации факта обращения за получением Сертификата, оформив Акт отказа от фотофиксации согласно Приложению № 6 к Регламенту или иной форме, полученной в УЦ или у Доверенного лица УЦ.

3.2.2. Заявитель обязан:

– при обращении в УЦ, в том числе по запросу УЦ, предоставлять достоверные сведения и документы, необходимые для осуществления функций УЦ;

– до обращения в УЦ ознакомиться с Регламентом и самостоятельно отслеживать его изменения на сайте УЦ;

– незамедлительно письменно информировать УЦ обо всех изменениях, относящихся к сведениям, представленным в УЦ;

– оплатить услуги УЦ.

3.3. Права и обязанности Пользователей

3.3.1. Пользователь-физическое лицо имеет право:

– осуществлять права, предоставленные Заявителям;

– получить СОС УЦ;

– получить Сертификат УЦ;

– применять Сертификат УЦ для проверки ЭП УЦ в Сертификатах, изготовленных УЦ;

– применять Сертификат для проверки ЭП;

– применять СОС УЦ для проверки статуса Сертификатов, изготовленных УЦ;

– обратиться в УЦ для прекращения действия Сертификата;

– обратиться в УЦ за подтверждением подлинности ЭП, созданных с использованием выданных УЦ Сертификатов, в электронных документах;

– получить копию полученного им в форме электронного документа Сертификата на бумажном носителе, заверенную УЦ;

– обратиться в УЦ за подтверждением подлинности ЭП УЦ в изготовленных им Сертификатах;

– сформировать ключи ЭП на своем рабочем месте с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным в соответствии с ФЗ «Об электронной подписи»;

– осуществлять иные права, предусмотренные действующим законодательством и Регламентом.

3.3.2. Пользователь-физическое лицо обязан:

– выполнять обязанности Заявителя;

– в период пользования услугами УЦ, в том числе по запросу УЦ, предоставлять достоверные сведения и документы, необходимые для осуществления функций УЦ;

– с целью обеспечения гарантированного ознакомления с изменениями и дополнениями Регламента до вступления их в силу не реже одного раза в 10 (десять) календарных дней обращаться на сайт УЦ за сведениями об изменениях и дополнениях в Регламент;

– обеспечить конфиденциальность ключа ЭП, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования;

– использовать для хранения ключа ЭП ключевой носитель, поддерживаемый используемым средством ЭП и соответствующий требованиями законодательства и нормативных правовых актов Российской Федерации;

– не использовать ключ ЭП в случае его компрометации или угрозы его компрометации;

– немедленно обратиться в УЦ с заявлением на прекращение действия Сертификата при компрометации или угрозе компрометации соответствующего ему ключа ЭП;

– не использовать ключ ЭП, связанный с Сертификатом, заявление на прекращение действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи такого заявления в УЦ по момент времени официального уведомления о прекращении действия данного Сертификата;

– не использовать ключ ЭП, связанный с Сертификатом, который аннулирован или действие которого прекращено;

– использовать для создания и проверки квалифицированной ЭП, создания ключей квалифицированных ЭП и ключей их проверки средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с ФЗ «Об электронной подписи»;

– известить УЦ об изменениях в ранее представленных данных, указанных в заявлении на изготовление Сертификата, и по требованию УЦ в течение 5 (пяти) рабочих дней представить документы, подтверждающие изменения, а при необходимости по согласованию с УЦ провести внеплановую замену Сертификата;

– соблюдать руководство по обеспечению безопасности использования квалифицированной ЭП и средств квалифицированной ЭП;

– подписывать документы, оформляемые УЦ в рамках процедур получения Пользователем Сертификата и иных услуг УЦ, в том числе в электронной форме, если конкретный способ получения Сертификата и (или) договор (соглашение) с УЦ предусматривает подписание документов в электронной форме;

– обеспечивать незамедлительное уничтожение принадлежащих им ключей ЭП по истечении сроков их действия, применяя для этого прошедшие в установленном порядке процедуру оценки соответствия средства ЭП, в составе которых реализована функция уничтожения информации;

– нести иные обязанности, предусмотренные действующим законодательством и Регламентом.

3.3.3. Пользователь-юридическое лицо в связи с использованием им Сертификата, выданного ему до 01.09.2023, имеет права, предусмотренные

абзацами 3-11 подпункта 3.3.1 настоящего Регламента и обязанности, установленные абзацами 2-15 подпункта 3.3.2 настоящего Регламента.

4. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющего центра

4.1. Процедура создания ключей ЭП и ключей проверки ЭП

4.1.1. Порядок создания ключей ЭП и ключей проверки ЭП

Заявитель (Пользователь-физическое лицо) вправе создать необходимые для получения Сертификата ключ ЭП и ключ проверки ЭП самостоятельно или получить ключ ЭП и ключ проверки ЭП в УЦ.

Заявитель (Пользователь-физическое лицо) обязан при создании ключа ЭП и ключа проверки ЭП соблюдать правила пользования средствами криптографической защиты информации, согласованные с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (далее — приказ ФСБ России № 66).

О необходимости получения ключа ЭП и ключа проверки ЭП в УЦ Заявитель (Пользователь-физическое лицо) указывает (ставит соответствующую отметку) в Заявлении на создание и выдачу Сертификата. Форма соответствующего заявления приведена в Приложении №1 к настоящему Регламенту.

Заявители, которые получают изготовленные УЦ ключ ЭП и ключ проверки ЭП, регистрируются в Реестре УЦ.

УЦ создает для Заявителей (Пользователей-физических лиц) ключ ЭП и ключ проверки ЭП, предназначенные для создания и проверки квалифицированной ЭП, в соответствии с ч. 4 ст. 5 ФЗ «Об электронной подписи» с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с:

– правилами пользования указанным средством ЭП, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России № 66;

– требованиями, установленными постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» в отношении автоматизированного рабочего места УЦ, используемого для создания ключа ЭП и ключа проверки ЭП для Заявителя (Пользователя).

Созданные УЦ ключ ЭП и ключ проверки ЭП записываются на ключевой носитель Заявителя (Пользователя-физического лица) либо ключевой носитель, имеющейся у УЦ, который будет использоваться

Заявителем (Пользователем-физическим лицом), без сохранения ключевой информации на каком-либо ином носителе.

Предоставляемый Заявителем (Пользователем-физическим лицо) в УЦ ключевой носитель для записи ключевой информации должен:

- иметь тип устройства, входящий в перечень, определяемый УЦ;
- иметь действующий сертификат соответствия требованиям информационной безопасности.

Ключевой носитель, являющийся средством криптографической защиты информации и приобретенный в УЦ, с записанным на нем ключом ЭП и ключом проверки ЭП выдается Заявителю (Пользователю-физическому лицу) под роспись в документах УЦ по учету средств криптографической защиты информации.

4.1.2. Смена ключей ЭП УЦ

Срок действия ключа ЭП УЦ устанавливается в соответствии с средством УЦ и средством ЭП, с использованием которого данный ключ был сформирован. Начало периода действия ключа ЭП УЦ исчисляется с даты и времени его создания.

Срок действия Сертификата, соответствующего ключу ЭП УЦ, устанавливается уполномоченным федеральным органом.

Смена ключей ЭП УЦ осуществляется в плановом и внеплановом порядке.

4.1.3. Плановая смена ключей ЭП УЦ

Основанием для плановой смены ключей ЭП УЦ является истечение 1 (одного) календарного года с момента их создания.

Плановая смена ключей ЭП УЦ осуществляется на следующий рабочий день после истечения 1 (одного) года с момента их создания в следующем порядке:

- УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- УЦ изготавливает запрос на Сертификат, который направляется в уполномоченный федеральный орган;
- после получения от уполномоченного федерального органа нового Сертификата УЦ, Сертификаты, создаваемые УЦ, подписываются новым ключом ЭП УЦ;
- новый Сертификат УЦ размещается на официальном сайте УЦ с возможностью его скачивания Пользователями.

Старый ключ ЭП УЦ используется в течение своего срока действия для формирования СОС, созданных УЦ в период его использования для подписания Сертификатов.

Информирование Пользователей о плановой смене ключей ЭП УЦ осуществляется путем размещения соответствующей информации на сайте УЦ, содержащей ссылку на новый Сертификат УЦ. Новый Сертификат УЦ

может быть получен путем скачивания Пользователями с сайта УЦ по указанной ссылке.

4.1.4. Внеплановая смена ключей ЭП УЦ

Внеплановая смена ключей ЭП УЦ осуществляется в случаях компрометации ключа ЭП или угрозы его компрометации.

При этом ключ ЭП УЦ признается скомпрометированным в случаях нарушения его конфиденциальности или угрозы нарушения его конфиденциальности в следствие хищения, утраты, разглашения и других случаев, в результате которых ключ ЭП мог стать доступным несанкционированным лицам и (или) процессам.

К угрозам нарушения конфиденциальности ключа ЭП УЦ относятся следующие виды угроз:

- естественные угрозы, вызванные воздействиями на информационные системы УЦ объективных физических процессов или стихийных природных явлений;
- угрозы, вызванные ошибками или халатностью персонала УЦ, в том числе нарушение правил эксплуатации средств УЦ и средств ЭП, ввод ошибочных данных и т.д.;
- угрозы преднамеренных действий злоумышленников, в том числе проникновение в помещение, в котором находятся средства УЦ и ЭП УЦ, внедрение вирусов и т.д.

Внеплановая смена ключей ЭП УЦ осуществляется незамедлительно после установления факта компрометации ключа ЭП УЦ или угрозы его компрометации в порядке, предусмотренном для плановой смены ключей ЭП.

Новый Сертификат УЦ размещается на сайте УЦ с возможностью его скачивания Пользователями.

Уведомление Пользователей о внеплановой смене ключей ЭП УЦ осуществляется путем рассылки им уведомлений на их электронную почту, указанную в полученном им Сертификате, и публикации информации на сайте УЦ с указанием, что новый Сертификат УЦ размещен на сайте УЦ. Новый Сертификат УЦ может быть скачан Пользователями с сайта УЦ.

Одновременно с внеплановой сменой ключа ЭП УЦ прекращается действие всех Сертификатов, созданных УЦ с использованием этого ключа. Информация о них заносится в Реестр сертификатов.

4.1.5. Смена ключа электронной подписи владельца Сертификата

Срок действия ключа ЭП владельца Сертификата устанавливается эксплуатационной документацией на средство ЭП, использованное для создания этого ключа ЭП. Начало периода действия ключа ЭП владельца Сертификата исчисляется с даты и времени начала действия соответствующего Сертификата.

Смена ключей ЭП владельца Сертификата осуществляется в случаях, указанных в п.п. 1, 2, 4 ч. 6 и ч. 6.1 ст. 14 ФЗ «Об электронной подписи».

Для смены ключа ЭП Владелец Сертификата представляет в УЦ заполненное и подписанное заявление согласно Приложению №4 к Регламенту на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной ЭП. При этом, если смена ключа ЭП владельца Сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной ЭП владельца Сертификата.

Изготовление и выдача УЦ новых ключей ЭП производится в порядке, предусмотренном пп. 4.1.1 Регламента. Создание и выдача Сертификата в таком случае осуществляется на основании заявления на создание и выдачу Сертификата в порядке, предусмотренном п. 4.2 Регламента.

4.2. Процедура создания и выдачи Сертификатов

4.2.1. УЦ изготавливает Сертификаты в соответствии с требованиями, установленным ФЗ «Об электронной подписи», приказом ФСБ России от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» и рекомендациями (разъяснениями) уполномоченных государственных органов.

4.2.2. Создание и выдача Сертификата осуществляется УЦ по заявлению на создание и выдачу Сертификата.

4.2.3. Заявление на создание и выдачу Сертификата подается по форме УЦ и должно содержать:

- сведения о присоединении к настоящему Регламенту;
- просьбу к УЦ о создании Сертификата;
- сведения о Заявителе (Пользователе – физическом лице), необходимые для идентификации Заявителя (Пользователя – физического лица) и заполнения Сертификата;
- контактные данные Заявителя (Пользователя-физического лица);
- согласие Заявителя (Пользователя-физического лица) на обработку предоставляемых им персональных данных и направление сведений о выданном Сертификате в Единую систему идентификации и аутентификации.

При необходимости Заявление на создание и выдачу Сертификата может содержать дополнительные сведения, в том числе о получении (смене) в УЦ ключей электронной подписи.

Заявление на создание и выдачу Сертификата может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручной подписью, так и в форме электронного документа, подписанного Заявителем квалифицированной ЭП либо простой ЭП, ключ которой получен Заявителем 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 Заявителя, являющегося гражданином 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». Заявление на создание и выдачу Сертификата, подписанное квалифицированной ЭП или указанной в настоящем абзаце простой ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Заявителя. При этом правила определения лица, подписывающего электронный документ, по его простой ЭП, и другие условия ее использования, в том числе обязанность соблюдать конфиденциальность ключа простой ЭП, определяются правилами использования простой ЭП при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации.

Типовая форма заявления на создание и выдачу Сертификата приведена в Приложении №1 к настоящему Регламенту. За получением актуальных форм заявления на создание и выдачу Сертификата Заявитель (Пользователь-физическое лицо) обращается в УЦ или к его Доверенным лицам. Актуальную форму Заявления на создание и выдачу Сертификата УЦ определяет самостоятельно и по своей инициативе праве вносить в нее любые изменения без уведомления участников электронного взаимодействия. Использование факсимиле (клише подписи) для подписания Заявления на создание и выдачу Сертификата не допускается.

4.2.4. Заявление на создание и выдачу Сертификата и необходимые документы на бумажном носителе предоставляются в УЦ или Доверенному лицу УЦ лично Заявителем (Пользователем-физическим лицом).

Заявление на создание и выдачу Сертификата в электронной форме подается путем заполнения его в Информационной системе УЦ, а также путем подписания его в информационной системе Пользователя УЦ с передачей в информационную систему УЦ при наличии защищенных каналов связи между информационной системой Пользователя и информационной системой УЦ.

Одновременно с подачей заявления Заявитель (Пользователь-физическое лицо) ознакамливается и подтверждает факт ознакомления с настоящим Регламентом, Руководством по обеспечению безопасности использования квалифицированной ЭП и средств квалифицированной ЭП, дает согласие на обработку предоставляемых им персональных данных.

4.2.5. Для проверки достоверности документов и сведений, представленных Заявителем (Пользователем-физическим лицом), и заполнения Сертификата, УЦ запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные ч. 2.2 ст. 18 ФЗ «Об электронной подписи».

4.2.6. Идентификация Заявителя (Пользователя-физического лица) осуществляется при его личном присутствии на основе следующих документов:

- личность гражданина Российской Федерации устанавливается по основном документу, удостоверяющему личность;
- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;
- личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

Идентификация заявителя (Пользователя-физического лица) – гражданина РФ может осуществляться без личного присутствия с использованием усиленной квалифицированной электронной подписи при наличии у него действующего Сертификата, также путем предоставления заявителем (Пользователем-физическим лицом) 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 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

4.2.7. Для создания и выдачи Сертификата в УЦ Заявитель (Пользователь-физическое лицо) представляет документы и сведения по перечню согласно Приложению № 5 к Регламенту.

В случае, если для подтверждения сведений, вносимых в Сертификат, законодательством Российской Федерации установлена определенная форма, Заявитель (Пользователь-физическое лицо) представляет в УЦ документ соответствующей формы.

4.2.8. При приеме заявления на создание и выдачу Сертификата и прилагаемых к нему документов осуществляется проверка:

- полноты комплекта документов на создание Сертификата;
- соответствия сведений, указанных в заявлении на создание и выдачу Сертификата, представленным документам;
- соответствия значений полей запроса на Сертификат значениям полей Заявления на создание и выдачу Сертификата.

Если документ и (или) его копия не подписан, не соответствует установленным законодательством требованиям, имеет неясный текст, подчистки, приписки, иные неоговоренные исправления, признаки подделки, повреждения, УЦ вправе отказать в принятии такого документа и (или) такой копии.

При поступлении заявления на создание и выдачу Сертификата в электронной форме также осуществляется проверка действительности ЭП, которой оно подписано. В случае недействительности ЭП, которой подписано заявление на создание и выдачу Сертификата, или подписания указанного заявления ЭП другого лица, или видом ЭП, не предусмотренным настоящим Регламентом, такое заявление УЦ не принимается.

4.2.9. Если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем (Пользователем-физическим лицом) для включения в Сертификат, и заявитель (Пользователь-физическое лицо) идентифицирован УЦ, УЦ осуществляет процедуру создания и выдачи Сертификата. В противном случае, а также в иных случаях, предусмотренных п. 3.1.2. настоящего Регламентам, УЦ отказывает в выдаче Сертификата.

4.2.10. Сертификат создается с использованием средств УЦ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, путем обработки запроса на Сертификат.

При этом, в случае создания ключей ЭП УЦ, запрос на Сертификат формируется на технических средствах УЦ. Если Заявитель (Пользователь-физическое лицо) сформировал ключи ЭП самостоятельно, одновременно с заявлением на создание и выдачу Сертификата Заявителем (Пользователем-физическим лицом) представляется запрос на Сертификат.

4.2.11. Созданный УЦ Сертификат записывается УЦ на сертифицированный ключевой носитель, за исключением случаев поступления Заявления на создание и выдачу Сертификата в форме электронного документа, подписанного ЭП либо использования Заявителем (Пользователем-физическим лицом) имеющего действующее подтверждение ФСБ России соответствия установленным требованиям средства ЭП, документация на использование которого предусматривает запись Сертификата непосредственно на устройство, на котором оно установлено (далее – СКЗИ с хранением).

4.2.12. Пользователь под расписку ознакамливается с информацией, указанной в Сертификате, в соответствии с ч. 3 ст. 18 ФЗ «Об электронной подписи», в том числе может быть ознакомлен под расписку посредством простой ЭП Заявителя, ключ которой получен им при личном обращении в соответствии с правилами использования простой ЭП при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации Заявителя, являющегося гражданином 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. Такая расписка, подписанная квалифицированной ЭП или указанной в настоящем пункте простой ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Заявителя. При этом правила определения лица, подписывающего электронный документ, по его простой ЭП, и другие условия ее использования, в том числе обязанность соблюдать конфиденциальность ключа простой ЭП, определяются правилами использования простой ЭП при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации.

Пользователю предоставляется руководство по обеспечению безопасности использования квалифицированной ЭП и средств квалифицированной ЭП.

4.2.13. Записанный на ключевой носитель Сертификат выдается Пользователю УЦ или вручается Доверенным лицом УЦ. В случае поступления заявления на создание и выдачу Сертификата в форме электронного документа, подписанного ЭП, созданный Сертификат предоставляется Пользователю путем размещения в информационной системе УЦ, за исключением случаев, если запрос на Сертификат сформирован в СКЗИ с хранением.

В случаях, когда запрос на Сертификат сформирован в СКЗИ с хранением, или по просьбе Заявителя (Пользователя-физического лица) созданный Сертификат размещается в устройстве с установленным СКЗИ с хранением.

4.2.14. Создание и выдача Сертификата осуществляется не позднее 1 (одного) рабочего дня с момента получения УЦ документов и сведений, необходимых для изготовления Сертификата.

При наличии возможности для срочного изготовления и выдачи Сертификата, по предварительной договоренности между УЦ и Заявителем (Пользователем-физическим лицом) УЦ вправе сократить срок создания Сертификата до 3 (трех) часов.

4.2.15. При выдаче Сертификата УЦ в единую систему идентификации и аутентификации направляются сведения о выданном Сертификате. По желанию владельца Сертификата УЦ безвозмездно осуществляет его регистрацию в единой информационной системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

4.3. Подтверждение действительности ЭП, использованной для подписания электронных документов

4.3.1. УЦ осуществляет подтверждение действительности ЭП в электронном документе, если формат электронного документа с ЭП соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS). Решение о соответствии электронного документа с ЭП стандарту CMS принимает УЦ.

4.3.2. УЦ осуществляет проведение экспертных работ по подтверждению действительности усиленной ЭП в электронном документе по заявлению на подтверждение действительности ЭП в электронном документе.

4.3.3. Заявление на подтверждение действительности ЭП в электронном документе представляется по форме согласно Приложению № 3 к Регламенту.

Обязательным приложением к указанному заявлению является носитель, содержащий:

- Сертификат, с использованием которого необходимо осуществить подтверждение действительности ЭП в электронном документе, – в виде файла стандарта CMS;
- Электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение ЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭП этих данных (файл стандарта CMS).

4.3.4. Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению заключения по выполненной проверке составляет 5 (пять) рабочих дней с момента поступления в УЦ заявления на подтверждение действительности ЭП в электронном документе и оплаты данной услуги УЦ.

4.3.5. Проведение работ по подтверждению действительности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников УЦ.

4.3.6. В ходе подтверждения действительности ЭП в электронном документе осуществляется проверка действительности всех Сертификатов, включенных в последовательность проверки, от проверяемого Сертификата до Сертификата УЦ, выданного ему головным удостоверяющим центром, функции которого выполняет уполномоченный федеральный орган.

4.3.7. Результатом проведения работ по подтверждению действительности ЭП в электронном документе является заключение УЦ.

4.3.8. Заключение УЦ должно содержать:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке.

4.3.9. Отчет по выполненной проверке должен содержать:

– время и место проведения проверки;
– содержание и результаты проверки;
– обоснование результатов проверки.

4.3.10. Заключение УЦ по выполненной проверке составляется в произвольной форме в 2 (двух) экземплярах, подписывается всеми членами комиссии и заверяется печатью УЦ. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

4.4. Процедуры, осуществляемые при прекращении действия (аннулировании) Сертификата

4.4.1. УЦ прекращает действие Сертификата в случаях, предусмотренных ст. 14 ФЗ «Об электронной подписи».

При этом УЦ в соответствии с п. 4 ч. 6 ст. 14 ФЗ «Об электронной подписи» вправе также прекратить действие выданного им Сертификата в следующих случаях:

– компрометации или обоснованном подозрении в компрометации ключа ЭП УЦ;
– компрометации или обоснованном подозрении в компрометации ключа ЭП Пользователя;
– невыполнение владельцем Сертификата обязанностей, установленных законодательством Российской Федерации в области ЭП и Регламентом;
– получения информации об изменении указанных в Сертификате данных Пользователя;
– установления наличия в Сертификате недостоверных или неполных сведений;
– получения подтверждения факта смерти владельца Сертификата – физического лица;
– получение подтверждения факта внесения в единый государственный реестр юридических лиц записи о ликвидации владельца Сертификата - юридического лица по Сертификатам, выданным до 01.09.2023, в которых наряду с наименование юридического лица указан его работник;
– неоплаты услуги по изготовлению и выдаче Сертификата;
– случаях, предусмотренных иными статьями ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми ими в соответствии с ними нормативными правовыми актами.

4.4.2. УЦ признает Сертификат аннулированным, если:

– не подтверждено, что владелец Сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в Сертификате;
– установлено, что содержащийся в 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.

4.4.3. Заявление на прекращение действия Сертификата предоставляется владельцем Сертификата в УЦ или Доверенному лицу УЦ на бумажном носителе, а также может быть направлено в форме электронного документа, подписанного действующей квалифицированной ЭП владельца Сертификата, в том числе с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (далее – Единый портал). В случаях, когда действие Сертификата прекращается в связи с компрометацией соответствующего ему ключа ЭП, заявление на прекращение действия Сертификата в электронной форме не может быть подписано с использованием указанного ключа ЭП.

4.4.4. Заявление на прекращение действия Сертификата должно содержать:

- серийный номер Сертификата, дату начала и окончания действия Сертификата, наименование УЦ, причины прекращения действия 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 российского юридического лица: наименования юридического лица, основного государственного регистрационного номера и идентификационного номера налогоплательщика;
- в отношении иностранной организации: наименования организации и идентификационного номера налогоплательщика (при наличии).

При необходимости Заявление на прекращение действия Сертификата может содержать дополнительные сведения.

Типовая форма Заявления на прекращение действия Сертификата для физических лиц, не являющихся индивидуальными предпринимателями, приведена в Приложении № 2 к Регламенту.

4.4.5. Прием заявления на прекращение действия Сертификата на бумажном носителе, а также рассмотрение заявления о прекращении действия Сертификата, в том числе представленного в электронной форме, осуществляется в течение рабочего дня УЦ.

4.4.6. Полномочия владельца Сертификата на прекращение его действия проверяются путем его идентификации при личной явке либо проверки действительности усиленной квалифицированной ЭП, которой подписано заявление на прекращение действия Сертификата в электронной форме. Владелец Сертификата, в котором наряду с наименованием юридического

лица указан работник этого юридического лица, представляет также документ, подтверждающий наличие у него полномочий на обращение с соответствующим заявлением, за исключением случаев, если такой документ, действующий на момент обращения, был ранее уже представлен в УЦ.

4.4.7. В случае направления владельцем Сертификата заявления на прекращение действия Сертификата с использованием Единого портала принятое по такому заявлению решение УЦ в форме электронного документа, подписанного квалифицированной ЭП УЦ, размещается в личном кабинете соответствующего владельца Сертификата на Едином портале после проведения проверки действительности квалифицированной ЭП УЦ, которой такое решение подписано, и подтверждения ее действительности.

4.4.8. Срок внесения информации о прекращении действия или аннулировании Сертификата в Реестр сертификатов не может превышать 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пунктах 4.4.1-4.4.2 Регламента в качестве оснований для прекращения действия или аннулирования Сертификата, или в течение 12 (двенадцати) часов с момента получения УЦ соответствующих сведений.

4.4.9. До внесения в Реестр сертификатов информации об аннулировании Сертификата УЦ уведомляет его владельца об аннулировании Сертификата путем направления электронного документа по адресу его электронной почты или посредством информационной системы УЦ, в которой владелец Сертификата имеет личный кабинет.

4.4.10. После внесения в Реестр сертификатов информации о прекращении действия (аннулировании) Сертификата УЦ осуществляет информирование об этом всех Пользователей УЦ. Официальным уведомлением о факте прекращения действия (аннулировании) Сертификата является опубликование СОС, содержащего сведения о прекратившем действие (отозванном) Сертификате.

4.4.11. СОС выпускается УЦ не реже 1 (одного) раза в 24 (двадцать четыре) часа и публикуется на Сайте УЦ в информационно-телекоммуникационной сети «Интернет».

4.4.12. В случае прекращения действия или аннулирования Сертификата, УЦ дополнительно опубликует в точках распространения списков отозванных сертификатов обновленный СОС в течение 12 (двенадцати) часов после поступления в УЦ заявления о прекращении Сертификата или иных сведений о наличии оснований для прекращения действия или аннулирования Сертификата.

В случае прекращения действия Сертификата по истечении срока его действия информация о прекратившем действие Сертификате в СОС не заносится.

4.4.13. Информация о размещении СОС заносится в расширение CRL Distribution Point Сертификата.

4.4.14. В случае внесения в Реестр сертификатов информации о прекращении действия Сертификата по заявлению на прекращение действие

Сертификата, поступившему с использованием Единого портала, УЦ после этого также посредством единой системы межведомственного электронного взаимодействия направляет информацию о прекращении действия Сертификата на Единый портал.

4.5. Ведение Реестра сертификатов

4.5.1. УЦ осуществляет формирование и ведение Реестра сертификатов в течение всего срока своей деятельности в соответствии с требованиями ФЗ «Об электронной подписи» и принятыми в соответствии с ним нормативными правовыми актами.

4.5.2. Реестр сертификатов ведется в электронном виде и кроме информации, содержащейся в Сертификатах, включает также информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях прекращения их действия или аннулирования, а также иную информацию, подлежащую включению в указанный реестр в соответствии с требованиями нормативных правовых актов.

4.5.3. УЦ обеспечивает актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

Для предотвращения утраты сведений о Сертификатах, содержащихся в Реестре сертификатов, УЦ формирует его резервную копию.

4.5.4. Информация о Сертификате вносится в Реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

Информация о прекращении действия (отзыва) Сертификата вносится в Реестр сертификатов не позднее 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пп.пп. 4.4.1 – 4.4.2 Регламента в качестве основания для прекращения действия или аннулирования Сертификата, или в течение 12 (двенадцати) часов с момента получения УЦ соответствующих сведений.

Действие Сертификата прекращается (Сертификат считается аннулированным) с момента внесения записи в Реестр сертификатов.

4.5.5. До внесения в Реестр сертификатов информации об аннулировании Сертификата УЦ уведомляет его владельца об аннулировании Сертификата путем направления электронного документа по адресу его электронной почты или посредством информационной системы УЦ, в которой владелец Сертификата имеет личный кабинет.

4.5.6. УЦ обеспечивает в течение срока своей деятельности любому лицу в любое время, за исключением периода планового или внепланового технического обслуживания, безвозмездный доступ к Реестру сертификатов с использованием информационно-телекоммуникационной сети «Интернет».

4.6. Порядок технического обслуживания Реестра сертификатов

4.6.1. УЦ вправе проводить плановое техническое обслуживание Реестра сертификатов только в выходные и праздничные дни с таким расчетом, чтобы начало регламентных работ приходилось не ранее чем на 01:00 московского времени первого выходного (праздничного) дня, следующего за рабочим днем, а окончание регламентных работ приходилось не позднее чем на 13:00 московского времени последнего перед рабочим выходного дня.

4.6.2. Не менее чем за 7 (семь) календарных дней до начала проведения плановых работ по техническому обслуживанию Реестра сертификатов УЦ должен уведомить Пользователей о проведении таких работ с указанием точной даты и времени их начала и окончания путем размещения соответствующей информации на сайте УЦ.

4.6.3. В случае невозможности обеспечения доступа к Реестру сертификатов в связи с внеплановыми техническими работами, УЦ незамедлительно размещает информацию об этом и примерных сроках восстановления доступа на сайте УЦ.

5. Порядок исполнения обязанностей Удостоверяющего центра

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

5.1.1. Информирование Заявителей (Пользователей) 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, осуществляется УЦ путем размещения соответствующей информации на сайте УЦ, а также информирования об условиях и порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности использования ЭП и средств ЭП, при выдаче Сертификата.

5.2. Выдача по обращению заявителя (Пользователя) средств электронной подписи

5.2.1. По обращениям Заявителей (Пользователей) УЦ предоставляет им средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с ФЗ «Об электронной подписи», и обеспечивающие в соответствии с ч. 4 ст. 6 ФЗ «Об электронной подписи» возможность проверки всех усиленных квалифицированных ЭП в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной ЭП, или в случае, если электронный документ подписан несколькими усиленными квалифицированными ЭП.

5.2.2. Условия, стоимость и порядок предоставления Заявителям (Пользователям) средств ЭП определяются отдельными договорами УЦ.

5.2.3. Факт выдачи средств ЭП заносится УЦ в документы УЦ по учету средств криптографической защиты информации.

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

5.3.1. Актуальность информации, содержащейся в Реестре сертификатов, обеспечивается своевременным внесением УЦ в соответствии

с пп. 4.5.4 Регламента в Реестр сертификатов сведений о созданных Сертификатах, об их аннулировании или прекращении действия.

5.3.2. Защита информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий достигается путем:

– использования технических средств защиты информации;

– ограничения доступа в помещения, где размещены аппаратные средства УЦ;

– идентификации, аутентификации и разграничение доступа Пользователей и обслуживающего персонала к программным средствам УЦ и защищаемой информации;

– контроля несанкционированного доступа и действий Пользователей, обслуживающего персонала и посторонних лиц.

5.3.3. Для предотвращения утраты сведений о Сертификатах, содержащихся в Реестре сертификатов, УЦ формирует резервную копию Реестра сертификатов.

5.4. Обеспечение доступности Реестра сертификатов

5.4.1. УЦ обеспечивает доступность Реестра сертификатов с использованием информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания указанного реестра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

5.4.2. Доступ к Реестру сертификатов осуществляется безвозмездно на основании запроса с указанием информации, позволяющей идентифицировать Сертификат в Реестре сертификатов и лицо, обратившееся за сведениями из Реестра сертификатов. Выписка из Реестра сертификатов по каждому отдельному выданному Сертификату предоставляется на основании отдельного запроса.

5.4.3. Техническое обслуживание Реестра сертификатов осуществляется с предварительным уведомлением Пользователей и с учетом ограничений, установленных п. 4.6 Регламента.

5.5. Порядок обеспечения конфиденциальности созданных УЦ ключей ЭП

5.5.1. Конфиденциальность созданных УЦ ключей ЭП обеспечивается за счёт создания ключей ЭП на автоматизированном рабочем месте, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, находящемся в аттестованном помещении, доступ в которое ограничен, на сертифицированный ключевой носитель.

При этом ключ ЭП и ключ проверки ЭП Пользователя формируются УЦ непосредственно на сертифицированный ключевой носитель, без сохранения ключевой информации на каком-либо ином носителе УЦ.

5.5.2. Владельцам Сертификатов перед выдачей Сертификатов разъясняются условия и порядок использования ЭП и средств ЭП и меры, необходимые для обеспечения безопасности ЭП, в том числе о хранении носителя ключевой информации в месте, не доступном третьим лицам.

5.5.3. Ключи ЭП Пользователей используются в соответствии со сроками их действия, определенными в пп. 4.1.5 Регламента.

5.6. Осуществление регистрации Сертификата и лица, которому выдан Сертификат, в единой системе идентификации и аутентификации

5.6.1. При выдаче Сертификата УЦ направляет в единую систему идентификации и аутентификации сведения о выданном Сертификате.

5.6.2. По желанию лица, которому выдан Сертификат, УЦ при выдаче Сертификата безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

5.7. Предоставление доступа к информации, содержащейся в Реестре сертификатов.

5.7.1. Доступ к информации, содержащейся в Реестре сертификатов, осуществляется безвозмездно на основании запроса с указанием информации, позволяющей идентифицировать Сертификат в Реестре сертификатов и лицо, обратившееся за сведениями из Реестра сертификатов. Выписка из Реестра сертификатов по каждому отдельному выданному Сертификату предоставляется на основании отдельного запроса.

5.7.2. Срок предоставления УЦ сведений из Реестра сертификатов составляет не более 7 (семи) дней для направления информации почтовым отправлением и 24 (двадцати четырех) часов для направления посредством информационно-телекоммуникационной сети «Интернет».

5.7.3. Актуальная информация об аннулированных и прекративших действие Сертификатах доводится до Пользователей путем публикации не реже чем раз в сутки актуального СОС.

При этом в случае прекращения действия или аннулирования Сертификата, УЦ дополнительно опубликует в точках распространения списков отозванных сертификатов обновленный СОС в течение 12 (двенадцати) часов после поступления в УЦ заявления о прекращении Сертификата или иных сведений о наличии оснований для прекращения действия или аннулирования Сертификата.

Информация о размещении СОС заносится в Сертификат в поле CRL Distribution Point.

6. Иные положения

6.1. Конфиденциальность информации

6.1.1. Конфиденциальной является информация о:

– ключах ЭП Пользователей;

– персональная и корпоративная информация о Пользователях, хранящаяся в УЦ и не подлежащая непосредственной рассылке в качестве части Сертификата;

– ключах ЭП УЦ.

6.1.2. Информация, не являющаяся конфиденциальной, считается открытой информацией и может публиковаться по решению УЦ. Место, способ и время публикации открытой информации определяется УЦ.

6.1.3. Персональные данные, включаемые в Сертификаты и СОС, издаваемые УЦ, предоставляются третьим лицам в соответствии ФЗ «Об электронной подписи».

6.1.4 Персональные данные Пользователя обрабатываются в целях предоставления услуг УЦ с его согласия. Персональные данные обрабатываются в течение всего срока деятельности УЦ.

6.1.5 Пользователь согласен с Политикой в отношении обработки персональных данных УЦ и принимает ее.

6.1.6. УЦ имеет право раскрывать конфиденциальную информацию третьим лицам только с согласия стороны, к которой относится эта информация, и в случаях, установленных законодательством Российской Федерации.

6.2. Хранение информации в Удостоверяющем центре

6.2.1. Хранение обязательной к хранению УЦ информации осуществляется в течение срока деятельности УЦ в электронной форме, если иное не установлено действующим законодательством.

6.2.2. Документы на бумажном носителе, относящиеся к владельцу Сертификата, хранятся в течение срока действия Сертификата, а после прекращения его действия – не менее предусмотренного действующим законодательством Российской Федерации срока.

6.2.3. Хранение документального фонда УЦ осуществляется в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

6.2.4 Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой из числа сотрудников УЦ и назначаемой приказом руководителя УЦ.

6.3. Ответственность сторон Регламента

6.3.1. Стороны несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Регламенту в соответствии с действующим законодательством РФ и положениями Регламента.

6.3.2. При этом УЦ не несет ответственность за убытки Заявителя (Пользователя), возникшие в случаях:

– несвоевременного оповещения Пользователем о факте компрометации ключа ЭП, собственником которого он является;

– невыполнения Заявителем (Пользователем) своих обязательств по настоящему Регламенту;

– подделки, подлога либо иного искажения информации третьими лицами в принадлежащих им Сертификатах, либо иных бумажных и электронных документах, с которыми Заявитель (Пользователь) ведет электронную переписку;

– неправомерных действий третьих лиц или действия форс-мажорных обстоятельств;

– если убытки возникли в результате предоставления Заявителем (Пользователем) заведомо ложной информации, или непредставления информации или материалов (документов) УЦ в разумный срок по письменному или устному запросу УЦ, а также в случаях утаивания информации Заявителем (Пользователем);

– упущенной выгоды Заявителя (Пользователя), связанной с ненадлежащим исполнением УЦ своих обязательств, за исключением убытков, связанных с включением по вине УЦ недостоверной информации в созданный им Сертификат или в реестр выданных и аннулированных сертификатов, ведение которого осуществляется УЦ, либо несвоевременным внесением информации в указанный реестр;

– а также в иных случаях, если УЦ выполнил все требования действующего законодательства РФ и настоящего Регламента.

6.4. Разрешение споров

6.4.1 Все споры, возникающие между Сторонами Регламента, подлежат разрешению путем переговоров. Сторона Регламента, получившая от другой Стороны претензию, обязана в течение 30 (тридцати) календарных дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа и подтверждающих их документов.

6.4.2. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются для юридических лиц – в Арбитражном суде Нижегородской области, для физических лиц – в Нижегородском районном суде города Нижнего Новгорода.

7. Список приложений

Приложение №1: Форма заявления на создание и выдачу Сертификата
Приложение №2: Форма заявления на прекращение действия Сертификата
Приложение №3: Форма заявления на подтверждение действительности электронной подписи в электронном документе
Приложение №4: Форма заявления на смену ключа электронной подписи
Приложение №5: Перечень документов, представляемых для создания и выдачи Сертификата
Приложение №6: Форма Акта отказа от фотофиксации
Приложение№7: Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи
Приложение №8: Структура СОС УЦ.

QR - код

Приложение №1 к Регламенту
Форма Заявления на создание и выдачу Сертификата

Номер заявки

ЗАЯВЛЕНИЕ
на создание и выдачу Сертификата

_____
(Ф.И.О. полностью)

В соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяюсь к Порядку реализации функций удостоверяющего центра АО «Аналитический Центр» и исполнения им обязанностей и обязуюсь соблюдать все его положения.

Прошу изготовить квалифицированный сертификат ключа проверки электронной подписи (далее также — Сертификат) Удостоверяющего центра АО «Аналитический центр», в соответствии со следующими идентификационными данными:

Фамилия		Страна	
Имя		Субъект (регион)	
Отчество		Населенный пункт	
ИНН Владельца Сертификата		Адрес места жительства/регистрации	
СНИЛС Владельца Сертификата		Пол	
Гражданство		Серия и номер паспорта[1]	
Дата рождения		Дата выдачи паспорта	
Контактный адрес электронной почты		Наименование органа, выдавшего паспорт	
Контактный номер мобильного телефона		Код подразделения органа, выдавшего паспорт	

Получение в удостоверяющем центре ключа электронной подписи и ключа проверки электронной подписи	Требуется/Не требуется [2]

Настоящим подтверждаю, что ознакомлен с опубликованным в сети Интернет по адресу: www.uc-osnovanie.ru**:**

- Порядком реализации функций аккредитованного удостоверяющего центра АО «Аналитический Центр» (Регламентом) и исполнения его обязанностей
- Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Настоящим даю согласие:

- на обработку АО «Аналитический Центр» (ИНН 5260270696, находящееся по адресу: 105005, город Москва, улица Радио, дом 24, корпус 2, помещение 1П/6) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» своих персональных данных, а именно: фамилии, имени и отчества, фотографии, контактном(ых) телефоне(ах), адресе электронной почты, СНИЛС, ИНН, пола, гражданства, паспортных данных (серия и номер, код подразделения, дата рождения, дата выдачи паспорта, адрес места жительства/регистрации) с целью создания и выдачи Сертификата, и обслуживания в удостоверяющем центре АО «Аналитический Центр» как с использованием средств автоматизации, так и без использования таких средств, включая совершение с ними следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение и передачу в течении срока деятельности удостоверяющего центра;
- на направление сведений о выданном Сертификате в Единую систему идентификации и аутентификации (система, удостоверяющая личность лица, для пользования электронными госуслугами и сервисами), содержащем персональные данные, в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Заявитель _____ _____ «__» _____ 20__ г.
(подпись) (Ф.И.О. полностью)

[1] Или иного основного документа, удостоверяющего личность.
[2] Нужно подчеркнуть.

Приложение №2 к Регламенту

Форма заявления на прекращение действия Сертификата

Заявитель: физическое лицо

В Удостоверяющий центр
АО «Аналитический Центр»
ИНН 5260270696
info@uc-osnovanie.ru
https://uc-osnovanie.ru/

ЗАЯВЛЕНИЕ
на прекращение действия сертификата

Я, _____,
(Ф.И.О. полностью)

прошу прекратить действие сертификата ключа проверки электронной подписи со следующими данными:

Серийный номер сертификата	
Издатель сертификата	АО «Аналитический Центр»
Срок действия сертификата	Действителен с: Действителен по:
Фамилия Имя Отчество	
ИНН	
СНИЛС	
в связи с (указать причину: компрометация ключа ЭП и т.д).	

Владелец Сертификата _____ _____
(подпись) (Ф.И.О. полностью)

«____» _____ 20____г.

_____ч. _____мин.

Приложение №3 к Регламенту
Форма Заявления
на подтверждение действительности
электронной подписи в электронном документе

Заявление
на подтверждение действительности электронной подписи в электронном документе

_____
(полное наименование организации, включая организационно-правовую форму для ЮЛ, Ф.И.О. – для ФЛ)

_____ (используется ЮЛ)
(должность, Ф.И.О. полностью)

действующего на основании _____ (используется ЮЛ)

Прошу подтвердить действительность электронной подписи в электронном документе на основании следующих данных:

1) файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение действительности электронной подписи в электронном документе на прилагаемом к заявлению носителе;

2) файл, содержащий подписанный электронной подписью данные и значение электронной подписи, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи, на прилагаемом к заявлению носителе.

Наименование файла: _____
Контрольная сумма файла: _____
Алгоритм расчета контрольной суммы:_____

Действительность электронной подписи прошу подтвердить по состоянию на

«____:_____» «____»_____/_____.
(час) (минута) (день) (месяц) (год)

Ответ прошу направить на адрес: _____

_____ ✓ _____ _____
(должность, используется ЮЛ) (подпись) (Ф.И.О. полностью)

Приложение №4 к Регламенту
Форма Заявления
на смену ключа электронной подписи

Заявление
на смену ключа электронной подписи

_____
Ф.И.О. полностью

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

просит взамен ранее созданных ключа электронной подпись и ключа проверки электронной подписи, указанного в созданном удостоверяющим центром АО «Аналитический Центр» квалифицированном сертификате ключа проверки электронной подписи с серийным номером _____, изготовить новый ключ электронной подписи и ключ проверки электронной подписи.

_____ _____ «___» _____ 20 __ г.
(Ф.И.О. полностью) (подпись)

Перечень документов,
предоставляемых для создания и выдачи Сертификата.

Для создания и выдачи Сертификата в соответствии со статьями 17 и 18 ФЗ «Об электронной подписи» предоставляются следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

- заявление на создания и выдачу Сертификата;
- основной документ, удостоверяющий личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования;
- иные документы по запросу УЦ.

Приложение №6
Форма Акта об отказе от фотофиксации

Акт отказа от фотофиксации

Гор. _____ «___» _____202__

Комиссия в составе:
1._____
(Должность ФИО (полностью) работника обособленного подразделения/филиала)

2._____
(Должность ФИО (полностью) работника обособленного подразделения/филиала) *

в присутствии Заявителя _____,
(Ф.И.О.)
обратившегося за получением услуги по созданию сертификата ключа проверки электронной подписи (далее – сертификат), составила настоящий Акт об отказе от фотофиксации, предназначенный для создания объективного технического подтверждения факта обращения за
получением сертификата в офисе _____.
(Наименование обособленного подразделения/филиала)

Личность установлена, его идентификация произведена должным образом в соответствии с требованиями Порядка реализации функций Удостоверяющего центра и/или действующими правилами и инструкциями АО «Аналитический Центр» и действующего законодательства. Документ, удостоверяющий личность (паспорт гражданина РФ), проверен, признаков его подделки, недействительности, непригодности не обнаружено.

_____
(Должность работника обособленного подразделения/филиала)

_____/_____/
(Ф.И.О. работника обособленного подразделения/филиала) (подпись)

_____
(Должность работника обособленного подразделения/филиала)

_____/_____/
(Ф.И.О. работника обособленного подразделения/филиала) (подпись)

_____/_____/
(Ф.И.О., заполняется собственноручно Заявителем) (подпись)

* В случае, если второй сотрудник филиала/обособленного подразделения АО «Аналитический Центр» не может по каким-либо причинам присутствовать при составлении акта отказа от фотофиксации, то в качестве второго лица, подтверждающего отказ от фотофиксации, привлекается работник одного из доверенных лиц удостоверяющего центра АО «Аналитический Центр».

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

1. Настоящее Руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированным сертификатом ключа проверки электронной подписи (далее - сертификат), об условиях, рисках и порядке использования усиленной квалифицированной электронной подписи (далее – квалифицированная ЭП) и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной ЭП. При применении квалифицированной ЭП в информационных системах владельцу сертификата необходимо выполнять требования:

- 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 Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152, в части обращения со средствами криптографической защиты информации;

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66, в части эксплуатации средств криптографической защиты информации;

- эксплуатационной документации к средствам электронной подписи;

- приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации. Если владельцем сертификата является организация, то в ней должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств квалифицированной ЭП, назначены владельцы средств квалифицированной ЭП и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств.

2. При размещении средств вычислительной техники с установленными на них средствами квалифицированной ЭП:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной ЭП, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств квалифицированной ЭП, общесистемного и специального программного обеспечения

3.1. При использовании средств квалифицированной ЭП должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами: - длина пароля должна быть не менее 6 символов; - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.); - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.); - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях; - личный пароль пользователь не имеет права никому сообщать; - периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований: - не использовать нестандартные, измененные или отладочные версии операционных систем; - исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой; - исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек; - на средствах вычислительной техники с установленными средствами квалифицированной ЭП должна быть установлена только одна операционная система; - все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.); - режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень; - всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права; - необходимо предусмотреть меры, максимально ограничивающие доступ к: - системному реестру; - файлам и каталогам; - временным файлам; - журналам системы; - файлам подкачки; - кэшируемой информации (пароли и т.п.); - отладочной информации.

3.1.3. На средствах вычислительной техники необходимо: - организовать удаление (по окончании сеанса работы средств квалифицированной ЭП) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям; - исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий; - регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.4. В случае подключения технических средств с установленными средствами квалифицированной ЭП к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.1.5. Необходимо организовать и использовать: - систему аудита, организовать регулярный анализ результатов аудита; - комплекс мероприятий по антивирусной защите.

3.2. Запрещается: - осуществлять несанкционированное копирование информации, записанной на ключевых носителей; - разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации; - использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя; - вносить какие-либо изменения в программное обеспечение средств

квалифицированной ЭП; - записывать на ключевые носители постороннюю информацию; - оставлять средства вычислительной техники с установленными средствами квалифицированной ЭП без контроля после ввода ключевой информации; - использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена (необходимо немедленно обратиться в удостоверяющий центр с заявлением на прекращение действия сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи); - использовать ключ электронной подписи и соответствующий сертификат, заявление на прекращение действия которого подано в удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия сертификата; - использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого прекращено; - использовать для создания и проверки квалифицированных ЭП, создания ключей электронной подписи и ключей проверки электронной подписи несертифицированные в соответствии законодательством Российской Федерации средства электронной подписи; - удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной ЭП

4.1. Меры защиты ключей квалифицированной ЭП. Ключи квалифицированной ЭП при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной ЭП согласно технической и эксплуатационной документации к ним. Если владельцем сертификата является организация, то ключевые носители должны иметь маркировку с учетным номером, присвоенным заявителем. Ключи квалифицированной ЭП на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной ЭП. Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца сертификата.

4.2. Обращение с ключевой информацией и ключевыми носителями. Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме ключей проверки ЭП). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками. Носители ключевой информации должны использоваться только их владельцем и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.). Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной ЭП операций формирования и проверки квалифицированной ЭП, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами. На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности автоматизированного рабочего места с установленными средствами квалифицированной ЭП. С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах: - на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3 настоящего Руководства; - должно быть установлено только лицензионное программное обеспечение; - должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных; - должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.); - должны регулярно устанавливаться обновления операционной системы; - должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной ЭП 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 пользователя с рабочего места. В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной ЭП, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред владельцу сертификата, в том числе средства квалифицированной ЭП, журналы работы систем обмена электронными документами и так далее.

4.4. Участники электронного взаимодействия при использовании квалифицированной ЭП обязаны обеспечивать незамедлительное уничтожение принадлежащих им ключей квалифицированной ЭП по истечении сроков их действия. Для уничтожения квалифицированных ключей ЭП должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства квалифицированной ЭП, в составе которых реализована функция уничтожения информации.

Структура Списка отозванных сертификатов

Название	Описание	Пример содержания
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = наименование Удостоверяющего Центра O = Организация OU = Подразделение L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида Серийный номер сертификата (CertificateSerialNumber) Время обработки заявления на отзыв сертификата (Time) Код причины отзыва сертификата (Reson Code)
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012

Расширения СОС

Reason Code	Код причины отзыва сертификата	"0" Не указана "1" Компрометация ключа "2" Компрометация ключа Удостоверяющего Центра "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор Удостоверяющего Центра, на котором подписан СОС
CA Version	Объектный идентификатор сертификата издателя	V0.0
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС