УТВЕРЖДЕНО

приказом директора АО «КАЛУГА АСТРАЛ»

№ 39 от 30 10 2024 года

И.И. Чернин

ПОРЯДОК

реализации функций аккредитованного удостоверяющего центра АО «КАЛУГА АСТРАЛ»

и исполнения его обязанностей

(регламент)

2024 г.

Редакция 10.6

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Настоящий Порядок реализации функций аккредитованного удостоверяющего центра Акционерного общества «КАЛУГА АСТРАЛ» и исполнения его обязанностей (далее – Порядок/Регламент, Удостоверяющий центр/УЦ соответственно) устанавливается Удостоверяющим центром и определяет условия предоставления услуг Удостоверяющего центра.

Порядок разработан в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.11.2020 № 584 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей» и иными применимыми нормативно-правовыми актами.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Порядке используются следующие термины и определения:

Удостоверяющий центр (УЦ) – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ; 63-ФЗ).

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона № 63-ФЗ.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа, либо порождаться в процессе информационного взаимодействия.

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

Квалифицированная электронная подпись (далее – КЭП) – усиленная электронная подпись, соответствующая следующим признакам:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи, а также следующим дополнительным признакам:
- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.

Сертификат ключа проверки электронной подписи (далее также по тексту - СКПЭП/Сертификат) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи (далее также по тексту - квалифицированный сертификат / КСКПЭП) – сертификат ключа проверки электронной подписи, соответствующий требованиям Федерального закона № 63-ФЗ и иным принимаемым в соответствии с ним нормативным правовым актам, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

Пользователь УЦ – лицо, присоединившееся к Порядку в соответствии с п.1.2.1 Порядка.

Владелец сертификата ключа проверки электронной подписи (далее – Владелец) – лицо, которому в установленном порядке выдан Сертификат в соответствии с Федеральным законом № 63-ФЗ и настоящим Порядком.

Ключ электронной подписи (далее – Ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи.

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

Средства электронной подписи – шифровальные (криптографические) средства, соответствующие требованиям к средствам электронной подписи, утверждённым Приказом ФСБ России от 29.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра», используемые для реализации хотя бы одной из следующих функций:

- создание электронной подписи;
- проверка электронной подписи;
- создание ключа электронной подписи и ключа проверки электронной подписи.

Средства Удостоверяющего центра – программные и (или) аппаратные средства, используемые УЦ для реализации функций удостоверяющего центра и получившие подтверждение соответствия требованиям, утверждённым Приказом ФСБ России от 29.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

Корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

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

Вручение сертификата ключа проверки электронной подписи – передача уполномоченным сотрудником УЦ или Доверенного лица УЦ созданного этим удостоверяющим центром Сертификата его Владельцу.

Подтверждение владения ключом электронной подписи – получение Удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением Сертификата, владеет Ключом ЭП, который соответствует Ключу проверки ЭП, указанному таким лицом для получения Сертификата.

Заявитель – физическое лицо, обращающееся в Удостоверяющий центр для получения Сертификата. После создания Сертификата Заявитель становится Владельцем Сертификата.

Уполномоченный сотрудник Удостоверяющего центра – физическое лицо, являющееся сотрудником УЦ, наделенное полномочиями по созданию электронных подписей под выдаваемыми УЦ Сертификатами в электронной форме и формируемыми списками аннулированных сертификатов (сертификатов, действие которых прекращено), полномочиями по приёму и проверке документов Заявителей, идентификации личности Заявителей, вручению Ключей ЭП, Ключей проверки ЭП и Сертификатов, созданных УЦ а также иными полномочиями согласно настоящему Порядку.

Доверенное лицо Удостоверяющего центра – юридическое лицо или индивидуальный предприниматель, действующий на основании договора или соглашения с УЦ, наделенное полномочиями, предусмотренными ч. 4 ст.13 Федерального закона № 63-ФЗ.

Уполномоченный сотрудник Доверенного лица – физическое лицо, являющееся сотрудником доверенного лица УЦ и наделенное полномочиями по приёму и проверке документов Заявителей, идентификации личности Заявителей, вручению Ключей ЭП, Ключей проверки ЭП и Сертификатов, созданных УЦ, а также иными полномочиями согласно настоящему Порядку.

Партнер УЦ – юридическое лицо или индивидуальный предприниматель, осуществляющее распространение программного обеспечения, которое предполагает необходимость использования КЭП или функциональные возможности которого предполагают возможность обращения в УЦ Заявителем, при этом заключившее с УЦ договор.

Ключевой носитель – физический носитель определенной структуры, предназначенный для хранения ключевой информации (исходной ключевой информации), а при необходимости - контрольной, служебной и технологической информации.

Реестр сертификатов – реестр выданных и аннулированных УЦ Сертификатов (сертификатов, действие которых прекращено), включающий в себя информацию, содержащуюся в выданных этим УЦ Сертификатах, информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях такого прекращения и аннулирования.

Компрометация ключа электронной подписи – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых ключи электронной подписи могут стать доступными несанкционированным лицам и/или процессам.

Плановая смена ключа электронной подписи – смена Ключа ЭП, не вызванная компрометацией Ключа ЭП, производимая Пользователем УЦ.

Реестр Удостоверяющего центра – набор сведений и документов Пользователей УЦ в электронной и (или) бумажной форме, включающий в себя следующую информацию:

- реестр зарегистрированных Пользователей УЦ;
- реестр документов и сведений, необходимых для изготовления Сертификата;
- реестр Сертификатов;
- реестр заявлений на прекращение действия Сертификата;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе.

Список аннулированных сертификатов – электронный документ с электронной подписью Уполномоченного лица УЦ формата X.509 версии 2, включающий в себя список серийных номеров сертификатов ключей проверки подписи, которые на момент времени формирования данного списка были аннулированы (действие которых прекращено) до окончания срока их действия. Момент времени формирования списка аннулированных сертификатов определяется по значению поля «Действителен с» списка аннулированных сертификатов.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет регулирования Порядка

1.1.1. Порядок регламентирует реализацию функций Удостоверяющего центра, условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Удостоверяющего центра, Заявителя и Владельца сертификата, форматы данных, организационные мероприятия, направленные на обеспечение работы Удостоверяющего центра.

1.1.2. Любое заинтересованное лицо может ознакомиться с Порядком на сайте Удостоверяющего центра по адресу https://astral.ru.

1.1.3. Порядок распространяет свое действие на всех лиц, которые в силу настоящего Порядка, соглашения с УЦ или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Порядком.

1.1.4. В случае противоречия и/или расхождения названия какого-либо раздела настоящего Порядка со смыслом одного из его пунктов, считается доминирующим смысл и формулировки каждого конкретного пункта.

1.1.5. В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Порядку с положениями Порядка, считается доминирующим смысл и формулировки Порядка.

1.2. Присоединение к Порядку

1.2.1. Любое лицо, подавшее в УЦ заявление на изготовление Сертификата, считается присоединившимся к Порядку на основании статьи 428 Гражданского кодекса Российской Федерации. С момента присоединения Заявителя к настоящему Порядку, он полностью и безоговорочно соглашается со всеми условиями настоящего Порядка и приложений к нему.

1.2.2. Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром в рамках настоящего Порядка, направив в Удостоверяющий центр заявление на прекращение действия выданного ему Сертификата.

1.3. Изменения (дополнения) Порядка

1.3.1. Внесение изменений (дополнений) в Порядок, в том числе в приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

1.3.2. Уведомление заинтересованных лиц о внесении изменений (дополнений) в Порядок и/или о новой редакции Порядка осуществляется Удостоверяющим центром путем публикации дополнений (изменений) и/или новой редакции Порядка на сайте по адресу https://astral.ru.

1.3.3. Изменения (дополнения), вносимые Удостоверяющим центром в Порядок, кроме изменений (дополнений), вызванных изменениями законодательства Российской Федерации, а равно новая редакции Порядка вступают в силу и становятся обязательными для Сторон по истечении 10 (Десяти) календарных дней с даты публикации соответствующих дополнений (изменений) и/или новой редакции Порядка на сайте по адресу https://astral.ru.

1.3.4. Изменения (дополнения), вносимые Удостоверяющим центром в Порядок в связи с изменением законодательства Российской Федерации, а равно новая редакции Порядка вступают в силу одновременно с вступлением в силу соответствующих нормативных актов.

1.3.5. Неотъемлемой частью настоящего Порядка являются Формы сертификатов. Удостоверяющий центр вносит изменения в Формы сертификатов путем публикации их

обновленных версий по адресу https://astral.ru. Изменения в Формы сертификатов вступают в силу в порядке, установленном пунктами 1.3.3, 1.3.4 Порядка.

1.4. Сведения об Удостоверяющем центре

1.4.1. Акционерное общество «КАЛУГА АСТРАЛ», именуемое в дальнейшем «Удостоверяющий центр» или «УЦ», зарегистрировано на территории Российской Федерации в городе Калуге. Свидетельство о государственной регистрации № 6294 от 18 марта 1998 года. Свидетельство о внесении записи в Единый государственный реестр юридических лиц за основным государственным регистрационным номером 1024001434049 от 25 декабря 2002 года.

Удостоверяющий центр в качестве участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской Федерации на основании разрешительных документов на осуществление видов деятельности, связанных с предоставлением услуг аккредитованного удостоверяющего центра:

– лицензии УФСБ России по Калужской области № 1534 Н от 23.03.2020 г. на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– уведомления уполномоченного федерального органа об аккредитации Удостоверяющего центра.

1.4.2. Реквизиты Удостоверяющего центра:

Полное наименование: Акционерное общество «КАЛУГА АСТРАЛ»

Сокращенное наименование: АО «КАЛУГА АСТРАЛ»

ИНН/КПП: 4029017981/402901001

ОГРН: 1024001434049

Код по ОКВЭД: 64.20.12

Код по ОКПО: 48357148

Юридический адрес: 248023, г. Калуга, переулок Теренинский, д. 6

Фактический (почтовый адрес): 248000, г. Калуга, ул. Циолковского, д. 4.

1.4.3. Банковские реквизиты:

Банк: КАЛУЖСКОЕ ОТДЕЛЕНИЕ N8608 ПАО СБЕРБАНК г Калуга

БИК 042908612

р/с 40702810422240101362

к/с 30101810100000000612

1.4.4. Контактные телефоны call-центра, адреса электронной почты:

+7 (4842) 788-999 – г. Калуга;

+7 (495) 663-73-58 – г. Москва;

+7 (812) 309-29-23 – г. Санкт – Петербург;

+7 (800) 700-39-84 – бесплатный федеральный номер;

Факс: +7 (4842) 57-74-60;

Web-сайт: https://astral.ru;

Адрес электронной почты Удостоверяющего центра: ca@astral.ru

Адрес электронной почты Клиентской службы: client@astral.ru

1.4.5. Адреса обособленных подразделений (филиалов) Удостоверяющего центра размещены на сайте: https://astral.ru

1.4.6. Адрес точки публикации корневых сертификатов Удостоверяющего центра и списков аннулированных сертификатов (сертификатов, действие которых прекращено) Удостоверяющего центра: http://dp.keydisk.ru

1.4.7. Адрес службы штампов времени (TSP): http://ocsp.keydisk.ru/TSP/tsp.srf

1.4.8. Удостоверяющий центр осуществляет свою работу в круглосуточном режиме. Информация о времени посещения офисов Удостоверяющего центра предоставляется при обращении Заявителя по контактным данным, указанным в п. 1.4.4 настоящего Порядка, а также на официальном сайте Удостоверяющего центра https://astral.ru

1.5. Порядок информирования о предоставлении услуг Удостоверяющего центра

1.5.1. Информирование по вопросам предоставления услуг Удостоверяющего центра осуществляется при обращении Заявителя по контактным данным, указанным в п. 1.4.4 настоящего Порядка, а также путем опубликования информации на официальном сайте https://astral.ru

1.5.2. Информирование субъектов Удостоверяющим центром производится посредством направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром, посредством направления SMS-уведомлений на телефонный номер, представленный Заявителем в Удостоверяющий центр, и/или посредством размещения информации на сайте по адресу https://astral.ru

1.5.3. Адреса местонахождения, справочные телефоны, адреса электронной почты и официальных сайтов обособленных подразделений (филиалов) Удостоверяющего центра опубликованы на официальном сайте Удостоверяющего центра https://astral.ru

1.6. Стоимость услуг Удостоверяющего центра

1.6.1. УЦ предоставляет услуги на возмездной основе.

1.6.2. Стоимость, взаимные встречные предоставления и состав услуг могут определяться одним из следующих способов:

- прайс-листом, который публикуется на сайте УЦ в сети «Интернет» по адресу: https://astral.ru;

- в условиях заключаемых УЦ с Заявителями или Партнерами договоров.

1.6.3. Сроки и порядок расчетов за услуги, оказываемые УЦ, регулируются условиями договора между Заявителем и УЦ или между УЦ и Партнером УЦ.

1.6.4. Оплата услуг УЦ осуществляется в российских рублях наличными денежными средствами или безналичным расчетом путем перечисления денежных средств на расчетный счет УЦ, если иное прямо не предусмотрено соглашением с УЦ.

1.6.5. В случаях, когда условиями договора с Заявителем предусмотрены прямые взаиморасчеты с УЦ, УЦ осуществляет выставление счета стороне, присоединившейся к Порядку (Заявителю), за оказываемые согласно настоящему Порядку услуги с использованием общедоступных средств связи, таких как: электронная почта, факсимильная связь, почтовое отправление, если иное прямо не предусмотрено соглашением с УЦ.

1.6.6. В случае нарушения Заявителем условий настоящего Порядка в отношении оплаты услуг УЦ в полном объеме, последний имеет право приостановить исполнение обязательств или применить иные меры воздействия, предусмотренные договором с Заявителем, с соблюдением требований, предусмотренных действующим законодательством Российской Федерации. В этом случае риск возможных убытков Заявителя полностью ложится на Заявителя (п.1. ст. 406 части первой Гражданского Кодекса Российской Федерации).

1.6.7. Услуги УЦ считаются оказанными, если Пользователь УЦ не предъявил претензий в письменном виде по их качеству и объему в течение 5 (пяти) рабочих дней со дня их оказания, с обязательным предварительным уведомлением Удостоверяющего центра о предъявлении претензии по телефону, факсимильной связи, электронной почте или по почте.

2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

2.1. Создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) при его личном присутствии либо посредством идентификации заявителя с применением информационных технологий без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, либо путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2.2. Изготовление и выдача по запросам Пользователей УЦ заверенных копий Сертификатов на бумажных носителях.

2.3. Выдача по обращению Заявителя средств электронной подписи, содержащих Ключ ЭП и Ключ проверки ЭП (в том числе созданные удостоверяющим центром) или обеспечивающих возможность создания Ключа ЭП и Ключа проверки ЭП Заявителем.

2.4. Создание по обращениям Заявителей Ключей ЭП и Ключей проверки ЭП с гарантией обеспечения конфиденциальности Ключей ЭП.

2.5. Предоставление Заявителям возможности для самостоятельного создания Ключей ЭП и Ключей проверки ЭП с гарантией обеспечения конфиденциальности Ключей ЭП.

2.6. Ведение реестра выданных и аннулированных Сертификатов (Реестр сертификатов), в том числе включающего в себя информацию, содержащуюся в выданных Сертификатах, и информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях таких прекращения или аннулирования.

2.7. Проверка уникальности Ключей проверки ЭП в Реестре сертификатов.

2.8. Проверка по обращениям Пользователей УЦ действительности ЭП, Ключи проверки которых содержатся в Сертификатах, выданных УЦ, в Электронных документах.

2.9. Предоставление сведений об аннулированных Сертификатах и Сертификатах, действие которых прекращено, в том числе опубликование Реестра сертификатов по адресам, вносимым в соответствующее дополнение Сертификатов.

2.10. Предоставление иных услуг, связанных с использованием ЭП и средств ЭП.

2.11. Установление сроков действия Сертификатов.

2.12. Аннулирование выданных УЦ Сертификатов.

2.13. Осуществление в соответствии с правилами подтверждения владения Ключом ЭП подтверждение владения Заявителем Ключом ЭП, соответствующим Ключу проверки ЭП, указанному им для получения Сертификата.

2.14. Осуществление проверки ЭП по обращениям участников электронного взаимодействия.

2.15. Осуществление иной деятельности, связанной с использованием электронной подписи, а также выполнение иных функций, связанных с использованием ЭП, установленных действующим законодательством Российской Федерации с учетом положений Регламента.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. Права Удостоверяющего центра

3.1.1. Запрашивать у Заявителя документы для подтверждения любой содержащейся в Заявлении на выдачу Сертификата информации, а также документы, необходимые для разрешения противоречий между данными в Заявлении на выдачу Сертификата и данными в иных представленных документах.

3.1.2. Произвести фотофиксацию будущего владельца Сертификата в анфас со страницей паспорта, на которой размещена фотография, или с его заполненным заявлением на изготовление Сертификата. В случае отказа произвести фотофиксацию Удостоверяющий центр вправе потребовать предоставить письменный отказ, выполненный будущим владельцем Сертификата. Письменный отказ должен быть выполнен собственноручно и должен содержать ссылку на факт отказа от проведения фотофиксации, а также фамилию, имя, отчество, дату и расшифровку подписи. Шаблон отказа от проведения фотофиксации является Приложением № 6 к Порядку.

3.1.3. При наличии сомнений в отношении волеизъявления Заявителя на выдачу Сертификата, достоверности предоставленной информации и документов, пригласить Заявителя лично для подтверждения волеизъявления, представленной информации и документов.

3.1.4. Обрабатывать персональные данные Заявителя с использованием технических средств.

3.1.5. Не принимать документы, не соответствующие требованиям действующих нормативных актов Российской Федерации, требованиям Порядка и Профиля Сертификата.

3.1.6. Отказать в изготовлении Сертификата Заявителю: в случае непредставления документов, представления документов не в полном объеме согласно Регламенту или предоставления документов, подлинность которых вызывает обоснованные сомнения, а равно в случае невыполнения Заявителем обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, условиями Регламента, а также в случае подачи заявления на изготовление Сертификата, имеющего исправления, ошибки и/или приписки, не подтвержденные собственноручной подписью Заявителя.

3.1.7. В одностороннем порядке прекратить действие Сертификата Пользователя УЦ в случае невыполнения им обязанностей, указанных в разделе 4.3 Порядка, а также в случае появления достоверных сведений о том, что документы и сведения, представленные в соответствии с разделом 6.2.4 настоящего Порядка, не являются подлинными или не подтверждают достоверность всей информации, включенной в данный Сертификат, а также в случае, если услуга по созданию и выдаче данного Сертификата не была оплачена в установленном порядке.

3.1.8. В одностороннем порядке прекратить действие Сертификата Пользователя УЦ в случае получения предписания на выполнение данных действий от уполномоченных государственных органов власти с уведомлением Владельца Сертификата и указанием обоснованных причин.

3.1.9. Отказать в прекращении действия Сертификата Пользователя УЦ в случае ненадлежащего (с нарушением условий Регламента и/или действующего законодательства Российской Федерации) оформления соответствующего заявления на прекращение действия Сертификата.

3.1.10. Удостоверяющий центр вправе наделить третьих лиц (Доверенных лиц УЦ) полномочиями по приему заявлений на выдачу Сертификатов, а также вручению

Сертификатов от имени УЦ. При совершении порученных УЦ действий Доверенное лицо УЦ обязано идентифицировать Заявителя при его личном присутствии.

3.1.11. Выдавать Сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе.

3.1.12. Подтверждать достоверность сведений, перечисленных в пунктах 1 и 2 части 1 статьи 18 Федерального закона от 06.04.2011 No 63-ФЗ «Об электронной подписи» одним из следующих способов:

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

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

3)с использованием единой системы идентификации и аутентификации.

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

3.2. Обязанности Удостоверяющего центра

3.2.1. Запросить у Заявителя документы для подтверждения любой содержащейся в заявлении на выдачу Сертификата информации, а также документы, необходимые для разрешения противоречий между данными в заявлении на выдачу Сертификата и данными в иных представленных документах.

3.2.2. Не принимать документы, не соответствующие требованиям действующих нормативных актов Российской Федерации, требованиям настоящего Порядка.

3.2.3. Использовать для изготовления Сертификатов только Средства Удостоверяющего центра, сертифицированные в соответствии с действующим законодательством Российской Федерации.

3.2.4. Использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган. Аккредитованному удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

3.2.5. Использовать Ключ ЭП Удостоверяющего центра только для подписи издаваемых им квалифицированных Сертификатов и списков аннулированных сертификатов.

3.2.6. Принимать все необходимые меры по защите Ключа ЭП Удостоверяющего центра.

3.2.7. Предоставить Пользователю УЦ Сертификат Уполномоченного лица УЦ в электронной форме.

3.2.8. Вносить в создаваемые Сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами.

3.2.9. С использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных заявителем, в порядке, предусмотренном 63-ФЗ

3.2.10. Отказать Заявителю в создании Сертификата в случае, если не было подтверждено, что Заявитель владеет Ключом ЭП, который соответствует Ключу проверки ЭП, указанному Заявителем для получения Сертификата.

3.2.11. Отказать Заявителю в создании Сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения Сертификата ключа проверки электронной подписи.

3.2.12. Обеспечивать уникальность регистрационной информации, вносимой в Реестр Удостоверяющего центра и используемой для идентификации Заявителей.

3.2.13. Не разглашать (не публиковать) регистрационную информацию Пользователей УЦ, за исключением информации, вносимой в изготавливаемые Сертификаты, которая признается Заявителем общедоступной.

3.2.14. Обеспечить изготовление Сертификата Пользователя УЦ по его заявлению, в соответствии с форматом и порядком идентификации личности Заявителя, определенным в настоящем Порядке.

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

3.2.16. Обеспечить уникальность регистрационных (серийных) номеров изготавливаемых Сертификатов Пользователей УЦ.

3.2.17. Обеспечить уникальность значений Ключей проверки ЭП в изготовленных Сертификатах Пользователей УЦ.

3.2.18. Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.

3.2.19. Проводить публикацию списков аннулированных сертификатов (сертификатов, действие которых прекращено) не менее чем в двух точках публикации. Полные адреса точек публикации списков аннулированных сертификатов (сертификатов, действие которых прекращено) указывается в соответствующем поле Сертификата Пользователя УЦ. Обновление списков аннулированных сертификатов (сертификатов, действие которых прекращено) проводится УЦ по факту аннулирования (прекращения действия) любого Сертификата. Период времени с момента аннулирования (прекращения действия) Сертификата до момента публикации в точках публикации не превышает 12 (двенадцати) часов.

3.2.20. Прекратить действие Сертификата Пользователя УЦ по соответствующему заявлению, в соответствии с порядком, определенным в настоящем Порядке.

3.2.21. Прекратить действие Сертификата Пользователя УЦ в случае компрометации Ключа ЭП Уполномоченного лица УЦ, с использованием которого был издан Сертификат.

3.2.22. Официально уведомить о факте аннулирования (прекращении действия) Сертификата его Владельца. Официальным уведомлением о факте аннулирования (прекращении действия) Сертификата является размещение в точках публикации актуального списка аннулированных сертификатов (сертификатов, действие которых прекращено), содержащего сведения об аннулировании (прекращении действия) Сертификата.

3.2.23. Информировать в письменной форме Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

3.2.24. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в Реестре Сертификатов УЦ, в том числе информацию об аннулировании (прекращении действия) Сертификата Пользователя УЦ в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами, за исключением периодов планового и внепланового технического обслуживания.

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

Доступ к Реестру Сертификатов УЦ осуществляется с использованием формы, размещенной на сайте Удостоверяющего центра по адресу: https://certificate-registry.keydisk.ru/certificate.

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

3.2.27. Осуществлять выдачу копий Сертификатов в электронной форме и/или на бумажных носителях по обращениям Пользователей УЦ.

3.2.28. При выдаче Сертификата направить в Единую систему идентификации и аутентификации (далее – ЕСИА) сведения о лице, получившем Сертификат, в объеме, необходимом для регистрации в ЕСИА, и о полученном им Сертификате (уникальный номер Сертификата, даты начала и окончания его действия, наименование УЦ). Осуществлять по желанию Пользователя УЦ безвозмездную регистрацию в ЕСИА.

3.2.29. Отказать в прекращении действия Сертификата Владельцу сертификата, подавшему заявление на прекращение действия Сертификата, в случае если Сертификат уже аннулирован или прекратил свое действие по другим основаниям.

3.2.30. Отказать в прекращении действия Сертификата Владельцу сертификата, подавшему заявление на прекращение действия Сертификата, в случае если истек установленный срок действия Ключа электронной подписи, соответствующего Ключу проверки электронной подписи в сертификате.

3.2.31. Хранить предоставленные Заявителем документы, перечень которых определен в п. 6.2.4 Порядка, либо их надлежащим образом заверенные копии и (или) сведения из них в течение всего срока деятельности УЦ, если более короткий срок не предусмотрен

действующим законодательством Российской Федерации или в части, не противоречащей ему, настоящим Регламентом. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.2.32. В случае принятия решения о прекращении деятельности УЦ:

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

– передать в уполномоченный федеральный орган в установленном порядке реестр выданных УЦ Сертификатов;

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

3.2.33. Выполнять настоящий Порядок, установленный УЦ в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также Федеральным законом 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами.

3.2.34. В порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и 9 аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», УЦ обязан отказать такому лицу в проведении указанной идентификации.

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

3.2.35. При выдаче Сертификата по желанию лица, которому выдан Сертификат, безвозмездно осуществлять регистрацию указанного лица в ЕСИА.

3.2.36. Отказать Заявителю в выдаче Сертификата в случае, если полученные в соответствии с Федеральным законом № 63-ФЗ и настоящим Порядком документы и сведения не подтверждают достоверность информации, представленной Заявителем для включения в Сертификат, и УЦ не может установить личность Заявителя.

3.2.37. Прекратить действие Сертификата Пользователя УЦ в случае получения УЦ подтвержденной информации о смерти Владельца Сертификата – физического лица.

3.2.38. При выдаче Сертификата предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите

информации", физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

3.2.39. Не указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном удостоверяющему центру любым другим удостоверяющим центром.

3.2.40. Одновременно с выдачей квалифицированного сертификата предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

3.2.41. Предложить использовать шифровальные (криптографические) средства, указанные согласно Федерального закона от 27 июля 2006 года No 149-ФЗ «Об информации, информационных технологиях и о защите информации», физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети «Интернет»), и указать страницу сайта в информационно-телекоммуникационной сети «Интернет», с которой безвозмездно предоставляются эти средства. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети «Интернет» при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

3.2.42. Предоставлять безвозмездно любому лицу по его обращению, в соответствии с установленным Порядком, доступа к информации, содержащейся в Реестре сертификатов, в том числе информации об аннулировании Сертификата.

3.2.43. Прекращать действие Сертификатов по запросам Пользователей УЦ и в иных случаях, установленных Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Заявителем, а также настоящим Порядком. Услуга оказывается путём внесения сведений о прекращении действия в Реестр сертификатов.

3.2.44. Знакомить Заявителей под расписку с информацией, содержащейся в Сертификатах.

3.2.45. В одностороннем порядке аннулировать Сертификат Пользователя УЦ, если УЦ стало известно, что Владелец Сертификата не владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком Сертификате.

3.2.46. Незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа электронной подписи, не предусмотренных соглашением сторон, или возникновения у аккредитованного удостоверяющего центра обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа электронной подписи (при осуществлении аккредитованным удостоверяющим центром деятельности, предусмотренной частью 2.2 статьи 15 Федерального закона № 63-ФЗ).

3.2.47. Не наделять третьих лиц (Доверенных лиц УЦ) полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени УЦ.

3.2.48. Исполнять иные обязанности, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и иными нормативными актами.

3.3. Ответственность Удостоверяющего центра

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

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

– неисполнения или ненадлежащего исполнения обязанностей, предусмотренных действующим законодательством и настоящим Порядком.

3.3.2. УЦ не несет ответственность за невозможность применения Сертификата в случае, если такая невозможность возникла после создания Сертификата и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

3.3.3. За невыполнение или ненадлежащее выполнение обязательств по настоящему Порядку, УЦ несет ответственность перед Пользователем УЦ в размере и порядке, установленном действующим законодательством и договором между Заявителем и УЦ. В случае, если изготовление Сертификата осуществляется в рамках договора между УЦ и Партнером УЦ, УЦ несет ответственность перед Партнером УЦ в размере и порядке, установленном соответствующим договором.

3.3.4. УЦ (работник аккредитованного удостоверяющего центра, доверенные лица и их работники) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также Порядком.

4. ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СЕРТИФИКАТА

4.1. Обязанности Заявителя

4.1.1. Предъявить документы, удостоверяющие личность Заявителя в соответствии с пунктом 6.2.4 настоящего Порядка.

4.1.2. Обеспечить личную явку Заявителя в УЦ или в офис Доверенного лица УЦ при выборе способа идентификации заявителя при его личном присутствии.

4.1.3. В случае идентификации заявителя без его личного присутствия с использованием КЭП, подписать заявление на изготовление Сертификата действующей КЭП.

4.1.4. Представить в УЦ документы, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем. Перечень документов, необходимых для создания Сертификата, определяется с учетом положений пункта 6.2.4 настоящего Порядка.

4.1.5. Осуществлять иные действия, предусмотренные порядком и/или действующим законодательством Российской Федерации.

4.2. Права Владельца сертификата

4.2.1. Обратиться в УЦ с заявлением на изготовление, прекращение действия Сертификата.

4.2.2. Получить Сертификат Уполномоченного лица УЦ.

4.2.3. Получить Средство(а) электронной подписи, получившее(ие) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ, и неисключительную лицензию на право его использования (при выдаче программного или программно-аппаратного средства).

4.2.4. Получить от УЦ Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

4.2.5. Получать список прекративших действие (аннулированных) Сертификатов, выпущенных УЦ.

4.2.6. Применять список прекративших действие (аннулированных) Сертификатов, изготовленных УЦ, для установления статуса Сертификатов, изготовленных УЦ.

4.2.7. Применять Сертификат Пользователя УЦ для проверки ЭП электронных документов в соответствии со сведениями, указанными в квалифицированном сертификате Ключа проверки ЭП.

4.2.8. Получить копию Сертификата в электронной форме, находящегося в Реестре сертификатов УЦ.

4.2.9. Обращаться в УЦ за получением информации о статусе Сертификатов и их действительности на определенный момент времени.

4.2.10. Обращаться в УЦ за подтверждением подлинности ЭП в электронном документе, сформированной с использованием Сертификата, изданного УЦ.

4.2.11. Хранить Ключ ЭП, Ключ проверки ЭП и Сертификат на ключевых носителях, поддерживаемых используемым средством электронной подписи.

4.2.12. Получить копию Сертификата на бумажном носителе, заверенную УЦ.

4.2.13. Обращаться в УЦ за подтверждением подлинности электронной подписи уполномоченного лица УЦ в изготовленных им Сертификатах.

4.2.14. Пользоваться сервисами Службы актуальных статусов сертификатов и Службы штампов времени, доступ к которым предоставляется УЦ.

4.3. Обязанности Владельца сертификата

4.3.1. Исполнять все обязанности, предусмотренные пунктом 5.2 настоящего Порядка.

4.3.2. Обеспечивать конфиденциальность Ключей электронных подписей, в частности, не допускать использование принадлежащих Владельцу Ключей электронных подписей без согласия Владельца.

4.3.3. Не использовать Ключ ЭП и немедленно обратиться в УЦ, выдавший Сертификат, для прекращения действия этого Сертификата при наличии оснований полагать, что конфиденциальность Ключа ЭП нарушена.

4.3.4. Уведомлять Удостоверяющий центр о нарушении конфиденциальности Ключа электронной подписи, Сертификат которой выдан Удостоверяющим центром, в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.

4.3.5. Представлять регистрационную информацию в объеме, определенном положениями настоящего Порядка.

4.3.6. Нести ответственность за достоверность предоставленной регистрационной информации.

4.3.7. Применять для подписи электронных документов только действующий Ключ ЭП.

4.3.8. Не использовать Ключ ЭП, связанный с соответствующим ему Сертификатом, заявление на прекращение действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия Сертификата до момента времени официального уведомления УЦ о прекращении действия Сертификата, либо об отказе в прекращении действия.

4.3.9. Не использовать Ключ ЭП, связанный с соответствующим ему Сертификатом, действие которого прекращено (аннулирован).

4.3.10. Ознакомиться с информацией, содержащейся в его Сертификате, подтвердив этот факт предоставлением Расписки в соответствии с пунктом 6.2.7 настоящего Порядка.

4.3.11. В случае самостоятельного создания Ключа электронной подписи предоставить Удостоверяющему центру запрос на сертификат в формате, описанном в рекомендациях IETF RFC 2986 "PKCS #10: Certification Request Syntax Specification (2000)", IETF RFC 4491 "Using GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 6986 «GOST R 34.11-2012: Hash Function», RFC 7091 «GOST R 34.10-2012: Digital Signature Algorithm», RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012» с выполнением требований, предъявляемых к таким электронным документам используемыми Удостоверяющим центром Средствами удостоверяющего центра. Запрос на Сертификат должен содержать всю информацию, представляемую для включения в выдаваемый Сертификат, сведения о Средствах электронной подписи, использовавшихся для создания Ключа электронной подписи и Ключа проверки, и о Средствах электронной подписи, с которыми будет использоваться Сертификат.

4.3.12. Обеспечивать незамедлительное уничтожение принадлежащих ему ключей электронных подписей по истечении сроков действия данных ключей в отношении усиленных квалифицированных электронных подписей. Для уничтожения ключей

электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи (сертифицированные ФСБ РФ), в составе которых реализована функция уничтожения информации.

4.3.13. Осуществлять иные действия, предусмотренные Порядком и/или действующим законодательством Российской Федерации.

4.4. Ответственность Пользователя УЦ

4.4.1. Пользователь УЦ несет ответственность за достаточность применяемых им мер по защите Ключа ЭП от компрометации, потери, уничтожения, изменения или иного неавторизованного использования.

4.4.2. За невыполнение или ненадлежащее выполнение обязательств по настоящему Порядку, Пользователь УЦ несет перед УЦ ответственность в размере и порядке, установленном действующим законодательством и заключенным договором.

5. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

5.1. Права Участников электронного взаимодействия

5.1.1. Использовать Реестр сертификатов для проверки действительности Сертификатов, созданных и выданных Удостоверяющим центром.

5.1.2. Получить Сертификат Удостоверяющего центра.

5.1.3. Получить информацию о Сертификате, находящемся в Реестре сертификатов Удостоверяющего центра.

5.1.4. Применять Сертификат для проверки ЭП в электронных документах.

5.1.5. Обратиться в Удостоверяющий центр за проверкой действительности ЭП, созданной с помощью Сертификата, выданного Удостоверяющим центром.

5.1.6. При обращении за выдачей Сертификата получить информацию о рисках, связанных с использованием ЭП.

5.2. Обязанности Участников электронного взаимодействия

5.2.1. Обеспечивать конфиденциальность Ключей ЭП, в частности, не допускать использование принадлежащих им Ключей ЭП без их согласия.

5.2.2. Уведомлять Удостоверяющий центр, выдавший Сертификат, и иных участников электронного взаимодействия о нарушении конфиденциальности Ключа электронной подписи в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.

5.2.3. Не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

5.2.4. Использовать для создания и проверки ЭП, ключа проверки ЭП и ключа ЭП средства электронной подписи в соответствии с Федеральным законом № 63-ФЗ.

6. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

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

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

Ключ электронной подписи и Ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи создаются с использованием Средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, с выполнением требований в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи Заявителя.

Создание Ключей ЭП и Ключей проверки ЭП осуществляется одним из следующих способов:

1. Создание осуществляется в УЦ или Доверенным лицом УЦ, имеющим лицензию ФСБ на работу с шифровальными (криптографическими) средствами).

УЦ (Доверенное лицо УЦ) создает Ключи ЭП и Ключи проверки ЭП для Заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Ключ ЭП и Ключ проверки ЭП, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона 63-ФЗ создаются на специализированном рабочем месте аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, размещенном в аттестованном лицензированном помещении, доступ в которое ограничен, с использованием Средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, с соблюдением требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания Ключа ЭП и Ключа проверки ЭП для Заявителя.

Созданные таким образом Ключи ЭП и Ключи проверки ЭП записываются на ключевой носитель, который выдаётся Заявителю по окончании процедуры выдачи Сертификата под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

2. Создание осуществляется самостоятельно Заявителем.

Создание Ключей ЭП и Ключей проверки ЭП осуществляется Заявителем самостоятельно на своем рабочем месте, при этом Заявитель создает Ключ ЭП на своем рабочем месте с использованием предоставленных Удостоверяющим центром либо собственных Средств электронной подписи.

Заявитель создает Ключ ЭП и Ключ проверки ЭП в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом

ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный № 6382) с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. № 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный № 17350).

Запрос на изготовление Сертификата передается Заявителем в УЦ на отчуждаемом носителе.

6.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев Сертификатов об осуществлении такой смены

Плановая смена Ключей Удостоверяющего центра (Ключа ЭП и соответствующего ему Ключа проверки ЭП) выполняется не ранее, чем через 1 (Один) год и не позднее, чем через 1 (Один) год и 3 (Три) месяца после начала действия соответствующего Ключа. Основанием для плановой смены Ключей Удостоверяющего центра является истечение соответствующего срока или переход на использование новых стандартов ЭП и функции хеширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования ЭП.

Процедура плановой смены Ключей Удостоверяющего центра осуществляется в течение 1-го рабочего дня в следующем порядке:

1)Уполномоченное лицо Удостоверяющего центра формирует новый Ключ ЭП, соответствующий ему Ключ проверки ЭП и запрос на Сертификат;
2)Уполномоченное лицо Удостоверяющего центра передает запрос на Сертификат в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи (далее – УФО);
3)УФО изготавливает Сертификат на основании сведений, содержащихся в запросе на Сертификат;
4)УФО публикует изготовленный Сертификат УЦ на портале УФО;

5)Старый ключ ЭП Удостоверяющего центра используется в течение своего срока действия для формирования списков аннулированных сертификатов, издаваемых УЦ в период действия старого Ключа ЭП Удостоверяющего центра;

6)Уведомление Пользователей УЦ о проведении плановой смены Ключей Уполномоченного лица УЦ осуществляется посредством размещения информации на официальном сайте Удостоверяющего центра https://astral.ru, а так же в Точке публикации корневых сертификатов Удостоверяющего центра и списков аннулированных сертификатов (сертификатов, действие которых прекращено) Удостоверяющего центра в сети «Интернет» по адресу: http://dp.keydisk.ru;

7)После размещения уведомления о факте плановой смены Ключей Удостоверяющего центра Владельцам сертификатов необходимо установить на своих компьютерах новый сертификат Удостоверяющего центра.

6.1.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности: основания, процедуры и сроки осуществления смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев Сертификатов об осуществлении такой смены

При использовании Ключа электронной подписи Удостоверяющего центра существуют различные угрозы нарушения конфиденциальности.

Угроза, реализованная с использованием уязвимостей информационно-программной системы, называется атакой. Существует три основные категории атак:

- отказ в обслуживании;
- раскрытие информации;
- нарушение целостности.

Для предотвращения атак на Ключ электронной подписи Удостоверяющего центра реализован изолированный режим работы программно-аппаратного комплекса Удостоверяющего центра – комплекс организационно-технических мер, при выполнении которых нарушитель не располагает программно-аппаратными средствами взаимодействия с Удостоверяющим центром.

Реализованные меры защиты нацелены на предотвращение компрометации или угрозы компрометации Ключа электронной подписи Удостоверяющего центра.

Компрометация или угроза компрометации Ключа электронной подписи Удостоверяющего центра является основанием полагать, что конфиденциальность Ключа электронной подписи нарушена.

Под компрометацией Ключа электронной подписи понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых Ключ электронной подписи может стать доступными несанкционированным лицам и (или) процессам. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) Ключей электронной подписи;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

В случае компрометации или угрозы компрометации Ключа электронной подписи Удостоверяющего центра выполняется внеплановая смена соответствующего Ключа сразу, как только такой факт компрометации или угрозы компрометации обнаружен.

Процедура внеплановой смены Ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены таких Ключей, согласно подразделу 6.1.2 настоящего Порядка.

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

Одновременно со сменой Ключа электронной подписи Удостоверяющего центра прекращается действие всех Сертификатов, подписанных этим Ключом электронной подписи, с занесением сведений об этих сертификатах в Реестр сертификатов.

После выполнения процедуры внеплановой смены Ключа электронной подписи Удостоверяющего центра прекращается действие Сертификата Ключа проверки

электронной подписи, Ключ электронной подписи которого подвергнут процедуре внеплановой смены.

Перечень прекративших свое действие сертификатов подписывается предыдущим Ключом электронной подписи (подвергшимся процедуре внеплановой смены).

Удостоверяющий центр информирует Владельцев сертификатов, которые прекращают свое действие, о факте внеплановой смены Ключей Удостоверяющего центра посредством уведомления по электронной почте, указанной в Сертификате и размещения информации на официальном сайте Удостоверяющего центра: https://astral.ru.

После получения уведомления о факте внеплановой смены Ключей Удостоверяющего центра Владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых Сертификатов в соответствии с порядком, установленным подразделом 6.2 настоящего Порядка. Владельцы Сертификатов КЭП могут получить новый квалифицированный сертификат Удостоверяющего центра в реестре сертификатов, выданных УФО, на официальном сайте Удостоверяющего центра https://astral.ru, а так же в точке публикации корневых сертификатов Удостоверяющего центра и списков аннулированных сертификатов (сертификатов, действие которых прекращено) Удостоверяющего центра в сети «Интернет» по адресу: http://dp.keydisk.ru

6.1.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Владельца Сертификата

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

Заявление на смену Ключа ЭП составляется по форме, установленной Удостоверяющим центром. Образец заявления публикуется на сайте https://astral.ru.

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

В таком случае соответствующее Заявление должно быть подписано собственноручно и подано в УЦ Заявителем лично.

Процедура выдачи Сертификата и Ключа ЭП (при необходимости) Владельцу сертификата, в том числе в электронной форме, осуществляется в соответствии со статьей 18 Федерального закона 63-ФЗ.

6.2. Процедура создания и выдачи Сертификатов

6.2.1. Порядок подачи заявления на создание и выдачу Сертификатов

Создание и выдача Сертификата осуществляется Удостоверяющим центром на основании Заявления на выдачу Сертификата.

В отдельных случаях Удостоверяющий центр может предоставить Заявителю доступ к автоматизированной информационной системе (далее – АИС УЦ), где Заявитель сможет самостоятельно подготовить заявление на выдачу Сертификата в электронном виде, а также передать в Удостоверяющий центр электронные копии документов, при условии подтверждения их соответствия оригиналам в УЦ (Доверенному лицу УЦ).

6.2.2. Требования к заявлению на создание и выдачу Сертификатов

Форма заявления на изготовление Сертификата утверждается Удостоверяющим центром и размещена в Приложении № 1 к настоящему Порядку, а так же на сайте УЦ в сети «Интернет» по адресу: https://astral.ru Перечень сведений, подлежащих обязательному указанию Заявителем, определяется формой заявления на изготовление Сертификата УЦ. Актуальный бланк заявления на изготовление Сертификата УЦ определяет самостоятельно и вправе вносить в него любые изменения по своей инициативе без уведомления Участников электронного взаимодействия.

Заявление может быть оформлено как на бумажном носителе, согласно актуальной формы УЦ, подписанное Заявителем собственноручно, так и в электронном виде, подписанное следующими способами:

- при помощи усиленной квалифицированной электронной подписи, сертификат ключа проверки которой на момент подписания является валидным (срок действия Сертификата не истек, Сертификат не аннулирован, действие Сертификата не прекращено, конфиденциальность Ключа ЭП не нарушена);

- посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» и информации из государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных».

Способ подачи заявления на изготовление Сертификата (в электронном виде или на бумажном носителе) определяется УЦ в зависимости от способа изготовления Ключей ЭП и выдачи Сертификата в рамках договора согласно которому осуществляется изготовление Сертификата.

При оформлении заявления на изготовление Сертификата на бумажном носителе запрещается использование факсимиле (клише подписи). Собственноручное подписание Заявления на бумажном носителе должно производиться чернилами (пастой) синего цвета.

6.2.3. Порядок идентификации Заявителя

Идентификация Заявителя производится следующими способами:

6.2.3.1. При личном присутствии по основному документу, удостоверяющему личность.

Идентификация гражданина Российской Федерации осуществляется по основному документу, удостоверяющему личность – паспорту гражданина РФ.

Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства (при наличии официального перевода на русский язык, заверенного нотариусом или дипломатическими (консульскими) органами) или по иному документу, удостоверяющему личность гражданина иностранного государства, признаваемому таковым действующим законодательством.

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

6.2.3.2. Без личного присутствия Заявителя с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, выданного удостоверяющим центром, аккредитованным в соответствии с Федеральным законом № 63-ФЗ.

6.2.3.3. Без личного присутствия Заявителя путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ №149).

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в ФЗ №149, удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

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

6.2.4. Перечень документов и сведений, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи Сертификатов. Порядок предоставления необходимых документов

При получении ЭП Заявитель должен предоставить оригинал документа, удостоверяющего личность, соответствующий следующим требованиям:

1)документ не должен быть просрочен;

2)документ не должен быть поврежден или испорчен;

3)документ не может содержать неточности и орфографические ошибки.

При обращении в аккредитованный удостоверяющий центр Заявитель представляет следующие документы либо их надлежащим образом заверенные копии и (или) сведения:

1. Заявление на изготовление Сертификата по форме Приложения № 1;
2. Основной документ, удостоверяющий личность Заявителя;

3. Страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования Заявителя (Заявитель вправе по собственной инициативе представить копии документов, подтверждающих данные сведения);

4. Идентификационный номер налогоплательщика (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения).

Перечень документов и (или) сведений, необходимых для изготовления и выдачи Сертификата устанавливается действующим законодательством Российской Федерации в области использования электронной подписи.

Удостоверяющий центр выполняет свою обязанность по внесению в Сертификат только достоверной и актуальной информации путем сбора сведений и/или скан-копий документов, представленных Заявителем, а также путем запроса соответствующих сведений из информационных систем органов государственной власти, Социального фонда России, единой информационной системы нотариата.

Если для подтверждения каких-либо сведений, вносимых в Сертификат, действующим законодательством Российской Федерации установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

6.2.5. Порядок проверки достоверности документов и сведений, предоставленных заявителем

Удостоверяющий центр осуществляет проверку достоверности документов и сведений, представленных заявителем:

1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов, в соответствии с пунктом 6.2.4 настоящего Порядка;
2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Социального фонда России, единой информационной системы нотариата;
3) с использованием единой системы идентификации и аутентификации.

Для заполнения Сертификата в соответствии с частью 2 статьи 17 Федерального закона «Об электронной подписи» Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона «Об электронной подписи». В случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в Сертификат, и Удостоверяющим центром идентифицирован заявитель, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю Сертификата. В противном случае Удостоверяющий центр отказывает Заявителю в выдаче Сертификата.

6.2.6. Порядок создания Сертификата

Удостоверяющим центром в Сертификат вносится информация на основании заявления на выдачу Сертификата. Удостоверяющий центр проверяет данные в Заявлении на выдачу Сертификата на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

– факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно представляет;

– факт соответствия сведений, указанных в заявлении на выдачу Сертификата, представленным документам и, в необходимых случаях в соответствии с Федеральным законом № 63-ФЗ, информации, полученной из государственных реестров;

– факт отсутствия явных признаков подделки документов.

В случае внесения в Сертификат персональных данных Заявитель предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в заявление на изготовление Сертификата и подписывается Заявителем вместе с заявлением на изготовление Сертификата. Персональные данные, внесенные в Сертификат, становятся общедоступными в соответствии с Федеральным законом № 63-ФЗ.

Удостоверяющий центр на основаниях, предусмотренных действующим законодательством или настоящим Порядком, вправе отказать в создании Сертификата.

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

6.2.7. Порядок выдачи Сертификата

Порядок выдачи Сертификата осуществляется в соответствии с Федеральным законом № 63-ФЗ.

По окончании процедуры создания Сертификата Заявитель получает:

- Ключ ЭП и соответствующий ему Ключ проверки ЭП (в случае, если создание Ключей ЭП Пользователя УЦ осуществлялось непосредственно в УЦ (в офисе Доверенного лица УЦ);
- Сертификат;
- Копию Сертификата на бумажном носителе (по запросу);
- CD-диск с технической документацией (передается при необходимости; информация может записываться в виде файлов на электронный USB-flash носитель).

При получении Сертификата Заявителем уполномоченный сотрудник УЦ или Доверенного лица УЦ ознакамливает его с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами, установленными Постановлением Правительства от 25.01.2013 № «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг», при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие (расписка), подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

При необходимости Владелец сертификата может обратиться за получением Сертификата к любому Доверенному лицу УЦ. При вручении Сертификата уполномоченный сотрудник Доверенного лица УЦ обязан установить личность Владельца сертификата по основному документу, удостоверяющему личность Владельца сертификата, при его личном присутствии.

Одновременно с выдачей квалифицированного сертификата уполномоченный сотрудник УЦ или Доверенного лица УЦ предоставляет Владельцу сертификата руководство по обеспечению безопасности использования

квалифицированной электронной подписи и средств квалифицированной электронной подписи (далее – Руководство).

Руководство передается одним из следующих способов:

- на бумажном носителе,

- в электронном виде путем отправки на адрес электронной почты, указанный Владельцем сертификата,

- путем опубликования Руководства в точке публикации по ссылке: https://astral.ru/support/astral-et/.

6.2.8. Срок создания и выдачи Сертификата с момента получения Удостоверяющим центром соответствующего заявления, а также условия для досрочного создания и выдачи Сертификата Заявителю

Создание и выдача Сертификата производится в течение трех рабочих дней с момента подачи заявления на изготовление Сертификата, при условии подтверждения всех фактов соответствия сведений в заявлении на изготовление Сертификата согласно подразделу 6.2.4 настоящего Порядка.

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

6.3. Подтверждение действительности электронной подписи, используемой для подписания электронных документов

6.3.1. Требования к заявлению на подтверждение действительности электронной подписи. Перечень прилагаемых к заявлению документов

Подтверждение действительности ЭП в электронном документе, авторство или содержание которого оспаривается, осуществляется УЦ на основании представленного в письменной форме заявления. Формы заявлений на подтверждение действительности ЭП в электронном документе размещены в Приложениях № 4 и 5 к настоящему Порядку, а также на сайте УЦ в сети «Интернет» по адресу: https://astral.ru.

В представленном заявлении должна быть указана информация о дате и времени формирования ЭП в электронном документе.

Обязательным приложением к заявлению о подтверждении действительности ЭП в электронном документе является внешний носитель электронной информации, на котором записаны:

– исходный (неподписанный) файл электронного документа, к которому применялась ЭП;

– файл электронного документа, подписанный ЭП, авторство которого оспаривается.

6.3.2. Срок предоставления услуг по подтверждению действительности электронной подписи в электронном документе

Срок проведения работ по подтверждению действительности ЭП в электронном документе составляет 15 (пятнадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр и при условии поступления оплаты стоимости данных услуг на расчетный счет Удостоверяющего центра.

6.3.3. Порядок оказания услуги по подтверждению действительности электронной подписи в электронном документе

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

Проверка действительности ЭП включает в себя:

– определение сертификата или нескольких сертификатов, необходимых для проверки ЭП;

– проверка ЭП электронного документа с использованием каждого сертификата;

– определение даты формирования каждой ЭП в электронном документе;

– проверка действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром;

– проверка действительности сертификатов на текущий момент времени;

– проверка отсутствия сертификатов в списках аннулированных сертификатов (сертификатов, действие которых прекращено) - CRL.

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

Проверка ЭП под электронными документами, созданными не Удостоверяющим центром, при технической совместимости используемых средств Удостоверяющего центра производится при представлении правил документирования, в соответствии с которыми были созданы электронный документ и проверяемая ЭП. При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

6.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата

6.4.1. Основания прекращения действия или аннулирования Сертификата

Сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона № 63-ФЗ, а именно:

– в связи с истечением установленного срока его действия;

– на основании заявления Владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

– в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;

– в иных случаях, установленных Федеральным законом № 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и Владельцем сертификата.

Удостоверяющий центр признает квалифицированный сертификат аннулированным в следующих случаях:

– не подтверждено, что Владелец сертификата владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком Сертификате;

– установлено, что содержащийся в Сертификате Ключ проверки ЭП уже содержится в ином ранее созданном Сертификате;

– вступило в силу решение суда, которым установлено, что Сертификат содержит недостоверную информацию.

6.4.2. Порядок действий Удостоверяющего центра при прекращении действия Сертификата

Для осуществления прекращения действия Сертификата Пользователь УЦ может подать соответствующие заявление одним из следующих способов:

- на бумажном носителе, заверенное собственноручной подписью;

- в форме электронного документа, подписанного усиленной квалифицированной электронной подписью;

- в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (далее – Единый портал).

Формы заявлений на прекращение действия Сертификата для юридических и физических лиц размещены в Приложениях № 2 и 3 к настоящему Порядку соответственно, а также на сайте УЦ в сети «Интернет» по адресу: https://astral.ru.

Уполномоченный сотрудник УЦ или Доверенного лица УЦ при приеме заявления на прекращение действия Сертификата должно убедиться, что за прекращением действия Сертификата обращается Владелец сертификата.

Приём заявлений осуществляется в УЦ или Доверенным лицом УЦ в рабочие дни в рабочее время (не ранее 9:00 и не позднее 18:00 местного времени). Информация о прекращении действия Сертификата вносится в Реестр сертификатов. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

Срок внесения информации о прекращении действия или аннулировании Сертификата в Реестр сертификатов не может превышать 12 (двенадцать) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона № 63-ФЗ (пункты 6.4.1 и 6.4.2 настоящего Порядка), или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений.

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

6.5. Порядок ведения реестра Сертификатов

6.5.1. Формы ведения реестра Сертификатов

Формирование и ведение Реестра сертификатов осуществляется в порядке, установленном Федеральным законом № 63-ФЗ.

Ведение Реестра сертификатов включает в себя:

– внесение изменений в Реестр сертификатов в случае изменения содержащихся в нем сведений;

– внесение в Реестр сертификатов сведений о прекращении действия или об аннулировании Сертификатов.

Доступ к Реестру Сертификатов УЦ осуществляется с использованием формы, размещенной на сайте Удостоверяющего центра по адресу: https://certificate-registry.keydisk.ru/certificate.

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

Хранение информации, содержащейся в Реестре сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Хранение в Удостоверяющем центре всех выданных Сертификатов осуществляется постоянно в форме электронных документов.

Удостоверяющий центр обеспечивает защиту информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности. Формирование и ведение Реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

Для предотвращения утраты сведений о Сертификатах, содержащихся в Реестре сертификатов, формируется его резервная копия.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов.

Структура Реестра сертификатов формируется и ведется в соответствии с требованиями Федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

Удостоверяющий центр ведет перечень аннулированных сертификатов (сертификатов, действие которых прекращено) в электронной форме формата X.509 версии 2.

6.5.2. Сроки внесения информации о прекращении действия или аннулировании Сертификатов в Реестр сертификатов

Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификатов составляет не более 12 (двенадцати) часов с момента приема заявления на прекращение действия Сертификата или наступления иного события, предусмотренного в частях 6 и 6.1 статьи 14 Федерального закона № 63-ФЗ (пункты 6.4.1 и 6.4.2 настоящего Порядка).

Срок внесения информации о прекращении действия или аннулировании Сертификата в Реестр сертификатов не может превышать 12 (двенадцать) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона № 63-ФЗ (пункты 6.4.1 и 6.4.2 настоящего Порядка), или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

6.6. Порядок технического обслуживания Реестра сертификатов

6.6.1. Максимальные сроки проведения технического обслуживания

Максимальный срок планового технического обслуживания составляет 3 (три) часа.

Внеплановое техническое обслуживание проводится при появлении такой необходимости в оперативном режиме. Срок проведения внепланового технического обслуживания составляет 3 (три) часа. Срок проведения внепланового технического обслуживания может быть увеличен по объективным причинам.

Максимальные сроки проведения планового и внепланового технического обслуживания Реестра сертификатов не может превышать установленные сроки внесения информации в Реестр сертификатов.

6.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

Удостоверяющий центр информирует участников информационного взаимодействия о проведении технического обслуживания посредством размещения информации на официальном сайте Удостоверяющего центра: https://astral.ru

7. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

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

Удостоверяющий центр информирует Заявителя об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки, посредством ознакомления с «Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи», которое предоставляется Заявителю одновременно с выдачей Сертификата, а также путем размещения «Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» на официальном сайте УЦ: https://astral.ru

7.2. Выдача по обращению заявителя средств электронной подписи

УЦ по обращению заявителя выдает средства ЭП, отвечающие требованиям:

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

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

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

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

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание ЭП, содержание информации, подписание которой производится;

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

3) однозначно показывать, что ЭП создана.

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

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

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

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

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

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

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

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

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

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

Средства ЭП должны обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

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

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

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

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

- предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременным обнаружением фактов несанкционированного доступа к информации;
- предупреждением возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможностью незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянным контролем за обеспечением уровня защищенности информации;

– нахождением баз данных информации в контролируемой зоне, исключающей свободное пребывание посторонних лиц;

– использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

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

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

7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

Ключ электронной подписи является конфиденциальной информацией Владельца Сертификата. Владелец Сертификата обязан обеспечивать конфиденциальность Ключа электронной подписи, в частности, не допускать использование Ключа электронной подписи без его согласия.

В Удостоверяющем центре Ключ электронной подписи создается на автоматизированном рабочем месте, аттестованном на соответствие требованиям по безопасности информации, размещенном в помещении УЦ (или Доверенного лица УЦ при наличии у него лицензии ФСБ на работу с шифровальными (криптографическими) средствами), доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель. После окончания процедуры создания Ключа электронной подписи Заявитель забирает ключевой носитель с записанным на нем Ключом электронной подписи.

Для создания Ключа электронной подписи в УЦ используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.

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

Запрещается:

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

2)вносить какие-либо изменения в ПО СКЗИ;

3)осуществлять несанкционированное копирование ключевых носителей;

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

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

6)записывать на ключевые носители постороннюю информацию;

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

8)защищать ключи ЭП на ключевом носителе паролем (пин-кодом);
9) оставлять без присмотра ключи ЭП на ключевом носителе (на столе, подключенным к ПЭВМ и пр.);

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

При временном хранении ключей ЭП необходимо соблюдать следующие условия:

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

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

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

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

7.6. Осуществление регистрации квалифицированного Сертификата в Единой системе идентификации и аутентификации

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

7.7. Осуществление по желанию лица, которому выдан квалифицированный Сертификат, безвозмездной регистрации указанного лица в Единой системе идентификации и аутентификации

При выдаче Сертификата КЭП Удостоверяющий центр по желанию лица, которому выдан Сертификат КЭП, безвозмездно осуществляет регистрацию указанного лица в ЕСИА, с проведением идентификации Владельца при его личном присутствии.

7.8. Предоставление доступа к информации, содержащейся в Реестре сертификатов

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к реестру квалифицированных сертификатов. Обращение к Реестру осуществляется по адресу https://certificate-registry.keydisk.ru/certificate. Для получения доступа к Реестру выданных (прекративших действие, аннулированных) сертификатов заинтересованное лицо заполняет форму запроса.

Обработка запроса осуществляется в режиме «онлайн». Информация предоставляется заинтересованному лицу в форме электронного сообщения.

8. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ И СЕРТИФИКАТОВ

8.1.Сроки действия Ключей ЭП Удостоверяющего центра составляют 1 год и 3 месяца.

8.2.Начало действия Ключа ЭП Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего Сертификата.

8.3.Начало периода действия Ключей ЭП Удостоверяющего центра исчисляется с момента начала действия его КСКПЭП.

8.4.Срок действия КСКПЭП Удостоверяющего центра составляет не более 15 (Пятнадцати) лет.

8.5.Максимальный срок действия Ключа ЭП Заявителя устанавливается эксплуатационной документацией средства электронной подписи (системы криптографической защиты информации), с использованием которого такой Ключ создается. Начало периода действия Ключа ЭП Заявителя исчисляется с момента начала действия КСКПЭП, соответствующего данному Ключу.

8.6.Срок действия КСКПЭП, создаваемого Удостоверяющим центром для Заявителя, указывается в КСКПЭП и не может быть более срока, определенного требованиями, установленными эксплуатационной документацией на Средства электронной подписи и средства Удостоверяющего центра, прошедшими в установленном порядке процедуру соответствия требованиям, установленным в соответствии с частью 5 статьи 8 Федерального закона № 63-ФЗ, с использованием которых такой КСКПЭП создается.

9. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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

9.2.Обработка персональных данных в УЦ осуществляется в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных применимых нормативно-правовых актов, действующих на территории Российской Федерации.

9.3.Персональные данные, обрабатываемые УЦ (конкретный набор сведений о субъекте персональных данных), определяются формами заявлений (приложений), являющихся неотъемлемой частью настоящего Регламента.

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

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

9.6. Согласие на обработку персональных данных Заявителя может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Заявителя, при удовлетворении которого впоследствии УЦ аннулируются все выпущенные сертификаты данного Заявителя, при этом УЦ вправе не прекращать обработку персональных данных до окончания срока действия согласия.

9.7. Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации, установленного ч. 2 ст.15 Федерального закона № 63-ФЗ.

9.8. На основании Федерального закона № 63-ФЗ (ч. 1 ст. 15) Аккредитованный УЦ хранит следующую информацию: реквизиты основного документа, удостоверяющего личность Владельца сертификата - физического лица.

Хранение информации осуществляется в соответствии с ч. 1 ст. 15, ч. 7 статьи 13 Федерального закона № 63-ФЗ.

9.9.Архивному хранению в УЦ в электронном виде подлежат документы и (или) сведения, получаемые УЦ согласно настоящего Порядка и требований Федерального закона № 63-ФЗ с учетом установленных законом требований и ограничений.

10. ПРИЛОЖЕНИЯ

Приложение №1

QR – код*
*если информационной системой удостоверяющего центра предусмотрена его генерация

Аккредитованный Удостоверяющий центр
АО «КАЛУГА АСТРАЛ»

Заявление

физического лица на изготовление квалифицированного сертификата ключа проверки электронной подписи

Я, _____
(фамилия, имя, отчество Заявителя)

паспорт: серия _____ № _____ код подразделения _____ дата выдачи _____ г.

_____
(наименование органа, выдавшего документ)

дата рождения: _____ г., место рождения: _____

адрес регистрации: _____

прошу создать квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

Фамилия	
Имя, Отчество	
СНИЛС	
ИНН	
Страна / Область*	РФ
Населенный пункт*	
Улица, номер дома, корпус, офис\квартира (если имеется) *	
Контактный адрес электронной почты	
Идентификатор запроса на сертификат **	
Контактный номер мобильного телефона*	

* - данные поля не являются обязательными для заполнения, но могут быть заполнены по желанию заявителя,

**- данное поле заполняется автоматически и только в случае автоматизированного формирования бланка Заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи в информационной системе УЦ.

Настоящим, в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие АО «КАЛУГА АСТРАЛ» (юридический адрес: 248023, г. Калуга, пер. Теренинский, д. 6, почтовый адрес: 248000, г. Калуга, ул. Циолковского, д. 4) на обработку своих персональных данных: фамилия, имя, отчество, ИНН, СНИЛС, адрес регистрации, адрес электронной почты, пол. телефон, паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), фотоизображение заявителя с паспортом или с заполненным заявителем заявлением на изготовление Сертификата, сканированную копию паспорта с фотоизображением заявителя, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) с использованием средств автоматизации и без использования таких средств.

Даю согласие _____
(наименование и адрес лица, осуществляющего обработку персональных данных по поручению оператора)
на обработку вышеуказанных персональных данных на основании поручения оператора.

Настоящее согласие на обработку персональных данных дается в целях исполнения обязательств аккредитованного Удостоверяющего центра АО «КАЛУГА АСТРАЛ» по изготовлению квалифицированных сертификатов ключей проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Выражаю согласие на внесение указанных в настоящем заявлении данных в реестр сертификатов, обязанность по ведению которого возложена на удостоверяющий центр согласно ст. 13 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи». Я проинформирован и даю согласие на предоставление АО «КАЛУГА АСТРАЛ» любому лицу по его обращению информации, содержащейся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи, во исполнение обязанности, возложенной на удостоверяющий центр п. 3 ч. 2ст. 13 вышеупомянутого Федерального закона.

Соглашаюсь с передачей своих персональных данных, указанных выше, в единую систему идентификации и аутентификации (далее - ЕСИА), в объеме, необходимом для регистрации в ЕСИА, в целях исполнения требования ч. 5 ст. 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Настоящее согласие на обработку персональных данных вступает в силу со дня его подписания. Согласие на обработку персональных данных может быть отозвано мной в письменной форме. Согласие действует на срок действия договора и в течение срока деятельности аккредитованного Удостоверяющего центра АО «КАЛУГА АСТРАЛ» (ч. 2 ст. 15 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»).

Даю согласие на создание квалифицированного сертификата ключа проверки электронной подписи в соответствии со сведениями, указанными в настоящем заявлении. Достоверность данных сведений подтверждаю.

Я проинформирован, что с момента подписания настоящего заявления присоединяюсь к порядку реализации функций аккредитованного удостоверяющего центра АО «КАЛУГА АСТРАЛ» (далее – Регламент), подтверждаю, что ознакомлен с руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи, размещенным в сети «Интернет» по адресу: https://astral.ru. Полностью и безоговорочно соглашаюсь со всеми условиями Регламента и приложений к нему.

_____ _____

(подпись) (фамилия, инициалы)

____ _____ ____ года

Приложение № 2

Для юридических лиц

Аккредитованный Удостоверяющий центр
АО «Калуга Астрал»

Заявление

на прекращение действия сертификата ключа проверки электронной подписи юридического лица

Я, ____
(фамилия, имя, отчество)

паспорт серии ________ № ________________ выдан «____» ____________ 20 _____ года

____
(наименование органа, выдавшего документ)

в связи с ____
(причина прекращения действия Сертификата)

прошу прекратить действие сертификата ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер сертификата	
Дата начала действия сертификата	
Дата окончания действия сертификата	
Наименование юридического лица	
ИНН	
ОГРН	
Фамилия	
Имя, отчество	

__________________________ __________________________
(подпись) (фамилия, инициалы)

«_____ »___________ 20 ___ года

ЗАПОЛНЯЕТСЯ ДОВЕРЕННЫМ ЛИЦОМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- -

Настоящим подтверждаю, что Заявление на прекращение действия сертификата ключа проверки электронной подписи получено, личность Владельца Сертификата

____
(фамилия, имя, отчество Владельца Сертификата в родительном падеже)

идентифицирована, сведения, указанные в Заявлении проверены.

Доверенное лицо Удостоверяющего центра

__________________________ __________________________
(подпись) (фамилия, инициалы)

« _____» ___________ 20 ___ года

М.П.

Приложение №3

Для физических лиц

Аккредитованный Удостоверяющий центр
АО «КАЛУГА АСТРАЛ»

Заявление

на прекращение действия сертификата ключа проверки электронной подписи физического лица

Я, ____
(фамилия, имя, отчество)

паспорт серии ________ № __________ выдан « ___ » __________ 20 _____ года

____
(наименование органа, выдавшего документ)

в связи с ____
(причина прекращения действия Сертификата)

прошу прекратить действие сертификата ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер сертификата	
Дата начала действия сертификата	
Дата окончания действия сертификата	
Фамилия	
Имя, отчество	
ИНН	
СНИЛС	

______________________ ______________________________
(подпись) (фамилия, инициалы)

«____» ___________ 20____ года

ЗАПОЛНЯЕТСЯ ДОВЕРЕННЫМ ЛИЦОМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- -

Настоящим подтверждаю, что Заявление на прекращение действия сертификата ключа проверки электронной подписи получено, личность Владельца Сертификата

____
(фамилия, имя, отчество Владельца Сертификата в родительном падеже)

идентифицирована, сведения, указанные в Заявлении проверены.

Доверенное лицо Удостоверяющего центра ____________________ ________________________
(подпись) (фамилия, инициалы)

« ____» ___________ 20 ____ года

М.П.

Приложение №4

Для юридических лиц

Аккредитованный Удостоверяющий центр
АО «КАЛУГА АСТРАЛ»

Заявление

на подтверждение действительности электронной подписи в электронном документе

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

в лице _____
(должность, фамилия, имя, отчество руководителя юридического лица)

действующего на основании _____
(основание полномочий)

просит подтвердить подлинность электронной подписи в электронном документе и установить статус сертификата ключа проверки электронной подписи (действовал / не действовал) на момент подписания документа электронной подписью.

Приложение:

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе (регистрационный № носителя _____).
2. Файл, содержащий подписанные электронной подписью данные, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи (файл открепленной электронной подписи), на прилагаемом к заявлению носителе (регистрационный № носителя _____).
3. Время на момент наступления которого требуется установить подлинность электронной подписи и статус сертификата:

_____
(указать дату и время (день, месяц, год, час, минута))

_____	_____	_____
(Должность руководителя юридического лица)	(подпись)	(фамилия, инициалы)

« ____» _____ 20 ____ года

М.П.

Приложение № 5

Для индивидуальных предпринимателей (физических лиц)

Аккредитованный Удостоверяющий центр АО «Калуга Астрал»

Заявление

на подтверждение действительности электронной подписи в электронном документе

Я, _____

(фамилия, имя, отчество)

паспорт серии _____ № _____ выдан «____» _____ 20____ года

_____

(наименование органа, выдавшего документ)

прошу подтвердить подлинность электронной подписи в электронном документе и установить статус сертификата ключа проверки электронной подписи (действовал / не действовал) на момент подписания документа электронной подписью.

Приложение:

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе (регистрационный № носителя _____).
2. Файл, содержащий подписанные электронной подписью данные, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи (файл открепленной электронной подписи), на прилагаемом к заявлению носителе (регистрационный № носителя _____).
3. Время на момент наступления которого требуется установить подлинность электронной подписи и статус сертификата:

_____

(указать дату и время (день, месяц, год, час, минута))

_____ _____

(подпись) (фамилия, инициалы)

«____» _____ 20____ года

Приложение № 6

Аккредитованный Удостоверяющий центр

АО «КАЛУГА АСТРАЛ»

Расписка об отказе от проведения фотофиксации

Я, _____

(фамилия, имя, отчество)

отказываюсь от создания фотоизображения.

Претензий к процедуре выдачи Сертификата ключа проверки электронной подписи не имею.

_____ _____

(подпись) (фамилия, инициалы)

« ____ » ____ 20 ____ года