

УТВЕРЖДЕНО

приказом директора АО «КАЛУГА АСТРАЛ»

№ 20 от 1 сентября 2025 года



И.И. Чернин

ПОРЯДОК

реализации функций аккредитованного удостоверяющего центра
АО «КАЛУГА АСТРАЛ»
и исполнения его обязанностей
(регламент)

2025 г.

Редакция 10.8

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	5
1. ОБЩИЕ ПОЛОЖЕНИЯ	8
1.1. Предмет регулирования Порядка	8
1.2. Присоединение к Порядку	8
1.3. Изменения (дополнения) Порядка	8
1.4. Сведения об Удостоверяющем центре	9
1.5. Порядок информирования о предоставлении услуг Удостоверяющего центра	10
1.6. Стоимость услуг Удостоверяющего центра	10
2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)	12
3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	13
3.1. Права Удостоверяющего центра	13
3.2. Обязанности Удостоверяющего центра	14
3.3. Ответственность Удостоверяющего центра	19
4. ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СЕРТИФИКАТА	20
4.1. Обязанности Заявителя	20
4.2. Права Владельца сертификата	20
4.3. Обязанности Владельца сертификата	21
4.4. Ответственность Пользователя УЦ	22
5. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ	23
5.1. Права Участников электронного взаимодействия	23
5.2. Обязанности Участников электронного взаимодействия	23
6. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ	24
6.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей	24
6.2. Процедура создания и выдачи Сертификатов	28
6.3. Подтверждение действительности электронной подписи, используемой для подписания электронных документов	32
6.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата	33
6.5. Порядок ведения реестра Сертификатов	35
6.6. Порядок технического обслуживания Реестра сертификатов	36
7. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	37
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	37
7.2. Выдача по обращению заявителя средств электронной подписи	37
7.3. Обеспечение актуальности информации, содержащейся в Реестре сертификатов, ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий	38
7.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов	39
7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей	39
7.6. Осуществление регистрации квалифицированного Сертификата в Единой системе идентификации и аутентификации	40
7.7. Осуществление по желанию лица, которому выдан квалифицированный Сертификат, безвозмездной регистрации указанного лица в Единой системе идентификации и аутентификации	40

7.8. Предоставление доступа к информации, содержащейся в Реестре сертификатов	40
8. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ И СЕРТИФИКАТОВ	41
9. ПЕРСОНАЛЬНЫЕ ДАННЫЕ	42
10. УСЛОВИЯ ВЫПОЛНЕНИЯ ФУНКЦИЙ ДОВЕРЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	43
11. ПРИЛОЖЕНИЯ	44

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;
- 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 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требованиям 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 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требованиям 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 Владелецу.

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 Владелецем 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 редакция 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: 62.0

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 № 8608 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 контактными 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 контактными 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 № 63-ФЗ, 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 № 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 № 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 информации из единой биометрической системы в порядке, установленном Федеральным законом от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации». 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 статье 19 Федерального закона от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», 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 статье 19 Федерального закона от

29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», 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 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», 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, доступ 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 России 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 от 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 Ключу 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 также 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 доступным 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 Владелец 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 также 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 также 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.

В случае подачи заявления посредством использования программы для ЭВМ, правообладателем которой являются Удостоверяющий центр и/или Партнеры УЦ, и/или распространение которой осуществляется Партнером УЦ, бланки заявлений на изготовление Сертификата определяются условиями использования соответствующей программы для ЭВМ.

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 соответствии с Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

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 статье 19 Федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», 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. № 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». Согласие на обработку персональных данных составляется по форме, предусмотренной Приложением № 8 к Порядку, подписывается Заявителем и предоставляется 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 ознакомливает его с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку или посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами, установленными постановлением Правительства от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг», при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из 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 должен 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 Владелец заявлением 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 № 63-ФЗ «Об электронной подписи» и требованиям приказа ФСБ России от 27.12.2011 г. № 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-телекоммуникационной 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 России 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), формой согласия на обработку персональных данных, 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 № 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. УСЛОВИЯ ВЫПОЛНЕНИЯ ФУНКЦИЙ ДОВЕРЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

10.1. Лицо, присоединившееся к Регламенту, в том числе иным образом принявшее на себя обязательство по соблюдению требований Регламента, которое исходя из существа заключенных таким лицом договоров выполняет функции доверенного лица Удостоверяющего центра, наделяется полномочиями на выполнение соответствующих функций на условиях, предусмотренных приложением № 7 к Регламенту.

10.2. С момента присоединения к Регламенту лицо, указанное в п. 10.1 Регламента, признается Доверенным лицом Удостоверяющего центра, а соглашение, предусмотренное приложением № 7 к Регламенту, считается заключенным между Удостоверяющим центром и Доверенным лицом Удостоверяющего центра.

10.3. Положения настоящего раздела Регламента не подлежат применению в случае, если между Удостоверяющим центром и Доверенным лицом Удостоверяющего центра заключено соглашение об исполнении обязательств доверенного лица аккредитованного удостоверяющего центра любым иным образом, отличным от способа заключения такого соглашения, предусмотренного п. 10.1 Регламента.

11. 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 места жительства (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.

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. 2 ст. 13 вышеупомянутого Федерального закона.

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» и исполнения его обязанностей (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

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.

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.

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.

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, минуту))

(подпись)

(фамилия, инициалы)

« ____ » _____ 20 ____ года

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
____ ____ ____

Соглашение
об исполнении обязательств доверенного лица аккредитованного удостоверяющего
центра АО «КАЛУГА АСТРАЛ»

1. Термины и определения

Если иное не предусмотрено настоящим приложением термины, определения и сокращения, применяемые по тексту настоящего приложения, используются в значении, указанном в Регламенте.

Программные продукты для электронных вычислительных машин (далее – ПП) – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения, правообладателем которых является Общество с ограниченной ответственностью «АСТРАЛ-СОФТ» (ОГРН 1214000000092).

Информационный ресурс – один из определяемых Удостоверяющим центром сервисов, размещенных в информационно-телекоммуникационной сети «Интернет» по адресу <http://reg.astralnalog.ru/> или <https://new-lk.lc-etp.ru>, или по иному, определенному Удостоверяющим центром, адресу.

Используемый Доверенным лицом Информационный ресурс определяется в зависимости от выбранного Доверенным лицом тарифа на приобретение неисключительных срочных прав на распространение и/или использование соответствующих ПП.

Соглашение – настоящее приложение к Регламенту.

2. Предмет и общие условия соглашения

2.1. Удостоверяющий центр оказывает услуги по созданию Сертификатов Заявителям, которые являются пользователями ПП (далее по тексту Соглашения – Заявитель), а Доверенное лицо Удостоверяющего центра (далее – Доверенное лицо) осуществляет распространение и/или использование соответствующих ПП на основании лицензионного или сублицензионного договора или в силу иных законных оснований.

2.2. Доверенное лицо осуществляет возложенные на него полномочия с использованием Информационного ресурса. Удостоверяющий центр обеспечивает доступ к Информационному ресурсу.

Доверенное лицо предоставляет заверения, что лица, имеющие доступ к Информационному ресурсу, являются надлежаще уполномоченными сотрудниками, состоящими в трудовых отношениях с Доверенным лицом. Доверенное лицо несет ответственность за все действия, совершенные такими лицами с использованием Информационного ресурса и при исполнении обязательств по Соглашению.

2.3. Доверенное лицо обязуется допускать к исполнению обязательств, предусмотренных настоящим приложением, исключительно лиц, отвечающих одновременно следующим требованиям:

- 1) наличие трудовых отношений с Доверенным лицом;
- 2) наличие познаний в вопросах порядка исполнения обязательств Доверенным лицом согласно условиям Соглашения.

2.4. Любые действия Доверенного лица по передаче каких-либо данных из информационных систем Доверенного лица в Информационный ресурс признаются передачей Доверенным лицом таких данных непосредственно Удостоверяющему центру.

2.5. При оказании Удостоверяющим центром услуги по выдаче Сертификата, Доверенное лицо осуществляет следующие действия:

2.5.1. Принимает от Заявителя заявление на изготовление Сертификата.

2.5.2. Проводит идентификацию Заявителя при личном присутствии в соответствии с требованиями и в порядке, установленном 63-ФЗ, Регламентом, публикуемой Удостоверяющим центром в Информационном ресурсе документацией.

2.5.3. Устанавливает сведения о Заявителе, предусмотренные пунктом 1 части 1 и части 2 статьи 18 63-ФЗ, Регламентом, а также проверяет иные сведения и документы, предусмотренные Регламентом.

2.5.4. Проводит визуальную проверку соответствия подписи Заявителя в подписываемых Заявителем документах, перечень которых определяется Регламентом и документацией, размещаемой Удостоверяющим центром в Информационном ресурсе (включая регламент проверки документов), и личной подписи Заявителя в предъявленном им основном документе, удостоверяющем личность; в случае явного расхождения подписей в указанных документах, Доверенное лицо обязано отказать Заявителю в выдаче Сертификата.

2.5.5. Проверяет оригиналы документов и (или) надлежащим образом заверенные копии таких документов, в целях подтверждения достоверности сведений, предоставленных Заявителем.

При возникновении у Доверенного лица сомнений в подлинности документов, удостоверяющих личность гражданина, его представителя или представителя юридического лица, обратившихся за получением Сертификата, Доверенное лицо вправе отказать в выдаче Сертификата.

2.5.6. Изготавливает электронные копии предоставленных Заявителем документов.

Представленные Заявителем надлежащим образом заверенные копии документов, а также изготовленные в соответствии с абзацем первым настоящего пункта электронные копии передаются Доверенным лицом в Удостоверяющий центр путем их размещения в Информационном ресурсе.

2.5.7. Обеспечивает ознакомление Заявителей с содержанием Регламента, что удостоверяется подписью Заявителя в заявлении на изготовление Сертификата.

2.5.8. Осуществляет фотофиксацию Заявителя в анфас с заполненным заявлением на изготовление Сертификата в руках и передает полученное фото в Удостоверяющий центр посредством использования Информационного ресурса. Качество фотографии должно предоставить возможность сличения лица Заявителя и сведений о Заявителе, содержащихся в заявлении на изготовление Сертификата.

В случае отказа Заявителя от фотофиксации Доверенное лицо обязано получить от него письменный отказ по форме, утвержденной Регламентом.

2.5.9. При вручении Сертификата и/или при вручении Сертификата Удостоверяющим центром Доверенное лицо производит ознакомление Владельца сертификата с информацией, содержащейся в Сертификате, под расписку, в порядке, предусмотренном частью 3 статьи 18 63-ФЗ. Указанная расписка передается Доверенным лицом Удостоверяющему центру путем размещения в Информационном ресурсе.

2.5.10. Доверенное лицо предоставляет Владельцу сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи одним из способов, определенных Регламентом.

2.6. Передача Удостоверяющему центру оригиналов подписанных Заявителями документов и иных документов, предоставленных Заявителем, производится в течение 3 (трех) рабочих дней (если иной срок не указан в требовании Удостоверяющего центра) с даты получения письменного требования от Удостоверяющего центра, путем их направления по адресу: 248000, г. Калуга, ул. Циолковского, д. 4, или иному, указанному Удостоверяющим центром адресу.

При отправке документов Доверенное лицо обязуется оформлять реестры (описи) отправляемых документов и приобщать их к отправляемым документам. Направляемые документы должны иметь пометку «На хранение в архив».

Хранение оригиналов указанных документов осуществляется Доверенным лицом в течение 5 (пяти) лет, хранение расписок об ознакомлении с информацией, содержащейся в Сертификате, – в течение неограниченного срока, до момента их востребования Удостоверяющим центром.

Порядок передачи документов, предусмотренный условиями настоящего пункта, может быть изменен Удостоверяющим центром в одностороннем порядке, путем направления письменного уведомления в адрес Доверенного лица в срок не позднее, чем за 30 (тридцать) календарных дней до даты вступления соответствующих изменений в силу.

3. Права и обязанности сторон

3.1. Удостоверяющий центр обязан:

3.1.1. Осуществлять своевременное размещение в Информационном ресурсе и обеспечивать доступ сотрудников Доверенного лица к информации, необходимой для исполнения обязательств в рамках Соглашения.

3.1.2. Оказывать каждому обратившемуся посредством Доверенного лица Заявителю, услуги Удостоверяющего центра в соответствии с условиями Соглашения, Регламента и пользовательской документацией на соответствующие ПП.

3.2. Удостоверяющий центр вправе:

3.2.1. Осуществлять контроль за соблюдением Доверенным лицом процедуры идентификации Заявителя, исполнения иных обязательств, предусмотренных Соглашением, вручения Заявителям Сертификатов в соответствии с публикуемой в Информационном ресурсе информацией.

3.2.2. Осуществлять проверки, в том числе дистанционно, с применением программных средств, используемых для получения от Доверенного лица информации, соблюдение Доверенным лицом Регламента, а также очно, путем посещения мест исполнения Доверенным лицом обязательств по Соглашению. О планируемой проверке с посещением места исполнения Доверенным лицом обязательств по Соглашению Удостоверяющий центр извещает Доверенное лицо за 5 (пять) рабочих дней до даты проверки. При этом количество проверок и сроки их проведения определяются Удостоверяющим центром и с Доверенным лицом не согласовываются.

3.2.3. В удобной для Удостоверяющего центра форме осуществлять проверки достоверности предоставляемых Доверенным лицом в рамках Соглашения сведений.

3.3. Доверенное лицо обязано:

3.3.1. Исполнять обязанности Доверенного лица, установленные Соглашением, Регламентом, а также нормативными правовыми актами Российской Федерации.

Доверенное лицо обязано вести учет своих сотрудников, использующих доступ к Информационному ресурсу для целей исполнения обязательств по Соглашению.

3.3.2. Исполнять полномочия и обязательства, предусмотренные Соглашением, самостоятельно. Передача полномочий третьим лицам и привлечение третьих лиц к исполнению обязательств, предусмотренных Соглашением, не допускается.

3.3.3. Информировать Заявителей об условиях и о порядке использования электронных подписей и средств электронных подписей, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей.

3.3.4. Обеспечить полноту и достоверность предоставляемой Удостоверяющему центру в рамках Соглашения информации, в том числе, в электронных документах и документах на бумажном носителе.

3.3.5. Отказать в выдаче Сертификата в случае подачи заявления на изготовление Сертификата, содержащем ошибки и (или) подчистки, либо при наличии в заявлении на изготовление Сертификата исправлений, и (или) приписок, не заверенных собственноручной (либо электронной) подписью Заявителя.

3.3.6. Отказать в выдаче Сертификата, если Заявитель отказывается или уклоняется от проведения идентификации при его личном присутствии, когда это необходимо в целях подтверждения его волеизъявления, предоставленной информации и документов, или удостоверения его личности.

3.3.7. Отказать в оказании услуги по выдаче Сертификата в случае отказа Заявителя предъявить документы для идентификации личности и полномочий.

3.3.8. По первому требованию предъявить Удостоверяющему центру документы и/или сведения для проверки соблюдения Регламента, в том числе:

- комплекты заявительных документов, представленных Заявителем для выпуска Сертификата;
- фотоизображение Заявителя согласно требованиям Регламента/письменный отказ Заявителя;
- сведения о проведении идентификации Заявителя (фамилию, имя, отчество сотрудника Доверенного лица, дату, время и место проведения идентификации);
- расписку об ознакомлении Владельца сертификата с информацией, содержащейся в Сертификате.

Запрашиваемая информация и документы должны быть представлены в течение 24 (двадцати четырех) часов с даты получения соответствующего требования.

3.3.9. Соблюдать размещаемые Удостоверяющим центром в Информационном ресурсе документацию, разъяснения, регламенты и иную информацию.

3.3.10. Возместить Удостоверяющему центру ущерб, понесенный им при компенсации убытков, причиненных третьим лицам вследствие их доверия к информации, указанной в Сертификате, прием заявления на создание и выдачу которого и (или) вручение которого осуществлялось Доверенным лицом в рамках исполнения Соглашения, а также компенсации иного вреда третьим лицам, предусмотренного частью 3 статьи 13 63-ФЗ, при условии нарушения Доверенным лицом требований Соглашения.

3.4. Доверенное лицо отказывает в выдаче Сертификата, если Заявитель не предоставил заявление на изготовление Сертификата и иные документы, предусмотренные Соглашением, Регламентом и 63-ФЗ.

3.5. Доверенное лицо не вправе осуществлять действия по созданию ключей электронных подписей и запросов на Сертификаты в интересах Заявителей самостоятельно для целей исполнения обязательств по Соглашению.

4. Ответственность

4.1. Удостоверяющий центр несет ответственность перед Заявителями за ненадлежащее выполнение обязательств Удостоверяющего центра, предусмотренных Регламентом и законодательством в сфере электронной подписи.

4.2. Доверенное лицо несет ответственность перед Удостоверяющим центром за ненадлежащее выполнение обязательств, предусмотренных Соглашением и Регламентом, в соответствии с действующим законодательством Российской Федерации.

4.3. Стороны не несут ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Соглашению, если причиной этого стали обстоятельства, находящиеся вне их контроля (обстоятельства непреодолимой силы), к которым могут относиться: объявленная или фактическая война, гражданские волнения, изменения военно-политической ситуации, эпидемии, блокада, эмбарго, землетрясения, наводнения, пожар и другие стихийные бедствия, отключение электроэнергии, действия государственных органов, издание законов и иных нормативных актов, препятствующих выполнению принятых на себя обязательств и другие чрезвычайные и непредотвратимые обстоятельства.

Наступление и продолжительность действия обстоятельств непреодолимой силы должны быть подтверждены соответствующими компетентными органами.

Сторона, для которой сложилась невозможность исполнения обязательств по Соглашению вследствие обстоятельств непреодолимой силы, должна письменно известить о наступлении (прекращении) таких обстоятельств другую сторону не позднее 7 (Семи) календарных дней с момента их наступления (прекращения). В этих случаях срок выполнения Сторонами обязательств по Соглашению продлевается соразмерно времени, в течение которого действовали такие обстоятельства и (или) их последствия.

Стороны установили, что введение какой-либо юрисдикцией, государством, объединением государств, участниками какого-либо международного договора в отношении Российской Федерации, стороны, участника стороны, конечного бенефициара стороны, аффилированного лица стороны санкций, запретов, ограничений и тому подобных мер не является обстоятельством непреодолимой силы по Соглашению.

5. Обработка персональных данных

5.1. Стороны обеспечивают безопасность персональных данных и обязуются принимать все разумные меры для защиты информации, содержащей персональные данные, полученной друг от друга, от несанкционированного доступа третьих лиц в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных).

5.2. Настоящим Удостоверяющий центр в соответствии с ч. 3 ст. 6 Закона о персональных данных поручает Доверенному лицу при исполнении им своих обязанностей по Соглашению обработку персональных данных Заявителей (Владельцев сертификатов) и их представителей на следующих условиях:

5.2.1. В соответствии с Законом о персональных данных и в целях исполнения Соглашения Доверенное лицо обязано осуществлять обработку персональных данных Заявителей (Владельцев сертификатов) и их представителей, работников Удостоверяющего центра, осуществляющих коммуникацию с Доверенным лицом в рамках Соглашения, с соблюдением принципов и правил

обработки персональных данных, предусмотренных законодательством Российской Федерации, в том числе осуществлять уничтожение либо обезличивание обрабатываемых персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2.2. Доверенное лицо осуществляет обработку персональных данных Заявителей в целях исполнения Удостоверяющим центром договора на оказание услуг по изготовлению Сертификатов в соответствии с 63-ФЗ.

5.2.3. Доверенное лицо осуществляет обработку персональных данных Заявителей (Владельцев сертификатов) и их представителей в объеме, необходимом для проведения процедуры создания и выдачи Удостоверяющим центром Сертификатов и определенном Регламентом, а именно: ФИО, ИНН, СНИЛС, адрес электронной почты, пол, телефон, паспортные данные (серия и номер, наименование органа/подразделения, выдавшего паспорт, код подразделения, место и дата рождения, дата выдачи паспорта, адрес места жительства (регистрации)), фотоизображение Заявителя с заполненным Заявителем заявлением на изготовление Сертификата, сканированная копия страницы/стороны паспорта, содержащей фотоизображение Заявителя.

5.2.4. Обработка персональных данных осуществляется Доверенным лицом путем совершения следующих операций с персональными данными (с использованием средств автоматизации или без использования таких средств): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение с использованием средств автоматизации и без использования таких средств, необходимых для исполнения Соглашения, достижения его целей с учетом ограничений, установленных законодательством.

5.2.5. Обработка персональных данных осуществляется Доверенным лицом с соблюдением конфиденциальности и обеспечением безопасности при обработке их для целей исполнения Соглашения в соответствии с требованиями законодательства Российской Федерации, а также с соблюдением требований к защите персональных данных, приведенных в ст. 19 Закона о персональных данных, и при необходимости – баз данных, находящихся на территории Российской Федерации.

5.3. Доверенное лицо обязуется: не раскрывать информацию о персональных данных субъектов персональных данных третьим лицам за исключением случаев, предусмотренных законодательством Российской Федерации; соблюдать требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Закона о персональных данных; по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора вышеуказанных требований; уведомлять оператора о случаях, предусмотренных частью 3.1 статьи 21 Закона о персональных данных.

5.4. Доверенное лицо несет ответственность перед Удостоверяющим центром за действия по обработке персональных данных Заявителей (Владельцев сертификатов) и их представителей в рамках поручения Удостоверяющего центра с момента получения персональных данных от субъекта персональных данных и до момента их уничтожения. В случае привлечения Удостоверяющего центра к ответственности за нарушение Доверенным лицом порядка обработки персональных данных, установленного Соглашением и Законом о персональных данных, Доверенное лицо обязуется возместить Удостоверяющему центру все причиненные убытки в том числе возместить денежные средства, выплаченные Удостоверяющим центром по требованиям субъектов персональных данных, и штрафы, выплаченные Удостоверяющим центром по постановлениям о привлечении к административной ответственности, вынесенным уполномоченными государственными органами, при условии и в случае, если действия Доверенного лица послужили основанием возникновения убытков у Удостоверяющего центра и подтверждены вступившим в силу судебным решением или постановлением о привлечении к административной ответственности, вынесенным уполномоченным государственным органом.

5.5. Иные непоименованные в Соглашении требования к защите обрабатываемых персональных данных, в том числе необходимые правовые, организационные и технические меры по защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении персональных данных определяются сторонами самостоятельно с учетом требований Закона о персональных данных.

5.6. Доверенное лицо подтверждает, что у лиц, получивших доступ к Информационному ресурсу, получены в установленном законом порядке согласия на обработку персональных данных,

в том числе для целей исполнения обязательств по Соглашению, включая их передачу Удостоверяющему центру.

6. Срок действия и порядок расторжения соглашения

6.1. Соглашение вступает в силу с даты, когда оно считается заключенным согласно условиям раздела 10 Регламента, и распространяет свое действие на правоотношения Удостоверяющего центра и Доверенного лица в течение всего срока распространения или использования Доверенным лицом ПП, если иное прямо не предусмотрено Договором на ПП.

6.2. Соглашение может быть расторгнуто досрочно по взаимному согласию сторон.

6.3. Любая из сторон вправе в одностороннем порядке отказаться от дальнейшего исполнения Соглашения, при письменном уведомлении другой стороны за 30 (тридцать) календарных дней до даты предполагаемого прекращения Соглашения. Соглашение считается прекращенным по истечении 30 (тридцати) календарных дней с даты отправки такого уведомления при условии доставки этого уведомления другой стороне.

Уведомление считается доставленным и в тех случаях, если оно поступило стороне, но по обстоятельствам, зависящим от нее, не было ей вручено или сторона не ознакомилась с ним.

6.4. Соглашение может быть досрочно расторгнуто Удостоверяющим центром в одностороннем порядке путем направления письменного уведомления в случае обнаружения нарушений Доверенным лицом условий Соглашения, Регламента или публикуемой в Информационном ресурсе документации, а также в случае, если Доверенное лицо перестало соответствовать требованиям к доверенным лицам.

Требования к Доверенным лицам и к лицам, допущенным для исполнения обязательств, предусмотренных Соглашением, устанавливаются Соглашением. Дополнительные требования могут размещаться Удостоверяющим центром на официальном сайте Удостоверяющего центра и/или доводиться до Доверенного лица иными предусмотренными Соглашением способами. В случае внесения изменений в требования, соответствующие изменения вступают в силу по истечении 10 (десяти) календарных дней с даты публикации соответствующих изменений на официальном сайте Удостоверяющего центра и/или с даты доведения таких изменений до Доверенного лица иными способами.

7. Урегулирование разногласий и рассмотрение споров

7.1. Все споры, возникающие в процессе исполнения Соглашения, будут разрешаться путем переговоров.

7.2. В случае если в ходе переговоров соглашение не достигнуто, заинтересованная сторона направляет претензию в письменной форме, подписанную уполномоченным лицом.

Претензия направляется любым из следующих способов:

- заказным письмом с уведомлением о вручении;
- курьерской доставкой. В этом случае факт получения претензии необходимо подтвердить распиской получающей стороны (далее – «Адресат»). Расписка должна содержать наименование документа и дату его получения, а также фамилию, инициалы, должность и собственноручную подпись лица, получившего данный документ.

Претензия считается доставленной, в том числе в случаях если она:

- поступила Адресату, но по зависящим от него обстоятельствам не была вручена или Адресат не ознакомился с ней;
- доставлена по адресу места нахождения сторон, даже если Адресат не находится по данному адресу.

К претензии должны быть приложены документы, обосновывающие предъявленные заинтересованной стороной требования (в случае отсутствия таких документов у другой стороны). Указанные документы представляются в форме копий, заверенных направившей их стороной.

Сторона, которой направлена претензия, обязана рассмотреть полученную претензию и о результатах уведомить в письменной форме заинтересованную сторону в течение 10 (десяти) календарных дней со дня получения претензии.

7.3. В случае невозможности разрешения споров в претензионном порядке, а также в случае неполучения ответа на претензию в течение указанного выше срока, споры между сторонами будут разрешаться в Арбитражном суде Калужской области в соответствии с законодательством Российской Федерации.

8. Заключительные положения

8.1. Стороны пришли к соглашению о возможности использования электронного документооборота наравне с документами на бумажных носителях.

Обмен документами в электронном виде по телекоммуникационным каналам связи осуществляется через организации, обеспечивающие обмен открытой и конфиденциальной информацией по телекоммуникационным каналам в рамках электронного документооборота с применением усиленной квалифицированной электронной подписи.

Любое уведомление, которое одна сторона направляет другой стороне в соответствии с Соглашением, может быть направлено в форме электронного документа, подписанного усиленной квалифицированной электронной подписью отправителя, если иное не предусмотрено Соглашением. Уведомление вступает в силу в день получения его лицом, которому оно адресовано, если иное не установлено законом или Соглашением.

8.2. В предусмотренных Соглашением случаях Стороны допускают возможность осуществления взаимодействия путем отправки сообщений по электронной почте.

Для целей оперативного обмена информацией, связанной с исполнением обязательств по Соглашению, Удостоверяющий центр вправе использовать любой известный ему адрес электронной почты Доверенного лица, в том числе адрес электронной почты Доверенного лица, опубликованный на сайте Доверенного лица в сети «Интернет».

Доверенное лицо вправе использовать адрес электронной почты Удостоверяющего центра, указанный в Регламенте.

В случае обмена документами на бумажных носителях стороны договорились использовать адреса места нахождения сторон, указанные в соответствующих государственных реестрах (ЕГРЮЛ/ЕГРИП).

8.3. В рамках Соглашения Стороны не оказывают друг другу каких-либо коммерческих услуг, Соглашение не предполагает взаимных расчетов Сторон.

Условия Соглашения регулируют обязательства Доверенного лица в связи с наделением его правами, предусмотренными частью 4 статьи 13 63-ФЗ, с учетом заинтересованности Доверенного лица выполнять соответствующую функцию в своих интересах и интересах своих контрагентов.

Участники правоотношений в рамках Соглашения в равной степени заинтересованы в сотрудничестве, их обязательства носят встречный равноценный характер.

8.4. Настоящим Стороны констатируют, что Удостоверяющий центр наделяет Доверенное лицо полномочиями, предусмотренными частью 4 статьи 13 ФЗ, по осуществлению функций доверенного лица в рамках Соглашения, включая следующие полномочия:

- 1) идентификацию личности Заявителя;
- 2) прием и хранение оригиналов заявительных документов, полученных от Заявителей;
- 3) осуществление проверки представляемых Заявителем документов и сведений, перечень которых установлен Регламентом и/или действующим законодательством Российской Федерации в сфере электронной подписи;
- 4) обработку пакета предоставленных документов для установления подлинности документов, включая визуальную проверку предоставленных документов на предмет наличия явных подделок и исправлений, для выявления которых не требуется специальных навыков и технических средств;
- 5) проверку полноты и достоверности сведений, необходимых для изготовления Сертификата;
- 6) ознакомление владельца с информацией, содержащейся в Сертификате;
- 7) подписание/проставление отметок доверенного лица удостоверяющего центра в бланке заявления на прекращение действия Сертификата;
- 8) осуществление иных обязательств, возложенных на Доверенное лицо, как на доверенное лицо удостоверяющего центра согласно действующему Регламенту и условиям Соглашения.

Доверенное лицо наделяется указанными в настоящем пункте Соглашения полномочиями в силу заключения Соглашения (пункт 4 статьи 185 Гражданского кодекса Российской Федерации) на срок действия Соглашения с правом передоверия указанных полномочий лицам, состоящим с Доверенным лицом в трудовых отношениях.

Согласие на обработку персональных данных

Я, _____
(фамилия, имя, отчество субъекта персональных данных (полностью) (далее – Заявитель))
паспорт: серия _____ № _____ код подразделения _____ дата выдачи _____ г.
_____ (наименование органа, выдавшего документ)
дата рождения: _____ г., место рождения: _____

адрес места жительства (регистрации)*: _____

* Данное поле является обязательным для заполнения, если в заявлении физического лица (Заявителя) на изготовление квалифицированного сертификата ключа проверки электронной подписи заполнено поле «адрес места жительства (регистрации)». В случае, если в заявлении физического лица (Заявителя) на изготовление квалифицированного сертификата ключа проверки электронной подписи поле «адрес места жительства (регистрации)» не заполнено, то в настоящем документе данное поле может не заполняться.

Настоящим, в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие Акционерному обществу «КАЛУГА АСТРАЛ» (АО «КАЛУГА АСТРАЛ»; оператор) (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 электронной почты, пол, номер телефона (в случае указания номера телефона в заявлении физического лица на изготовление квалифицированного сертификата ключа проверки электронной подписи), паспортные данные (серия и номер, наименование органа/подразделения, выдавшего паспорт, код подразделения, место и дата рождения, дата выдачи паспорта, адрес места жительства (регистрации) (в случае указания адреса места жительства (регистрации) в заявлении физического лица на изготовление квалифицированного сертификата ключа проверки электронной подписи), фотоизображение Заявителя с паспортом или с заполненным Заявителем заявлением на изготовление квалифицированного сертификата ключа проверки электронной подписи, сканированная копия страницы/сторон паспорта, содержащей фотоизображение 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 на обработку вышеуказанных персональных данных на основании поручения оператора следующими лицами:

1) Общество с ограниченной ответственностью «АСТРАЛ-СОФТ» (ООО «АСТРАЛ-СОФТ») (юридический адрес: 248000, Калужская обл., г. Калуга, ул. Циолковского, д. 4, офис 211);

2) _____
(наименование и адрес лица, осуществляющего обработку персональных данных по поручению оператора)

3) _____
(наименование и адрес лица, осуществляющего обработку персональных данных по поручению 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 данных, указанных в представленном мной заявлении на изготовление квалифицированного сертификата ключа проверки электронной подписи, в реестр сертификатов, обязанность по ведению которого возложена на удостоверяющий центр (АО «КАЛУГА АСТРАЛ») 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. 2 ст. 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 правоотношений между мной и АО «КАЛУГА АСТРАЛ», связанных с изготовлением квалифицированного сертификата ключа проверки электронной подписи, 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»).

« ____ » _____ 20 ____ года

(подпись)

(фамилия, инициалы субъекта персональных данных)