УТВЕРЖДАЮ
Генеральный директор
АО «ПФ «СКБ Контур»

_____ Е. Ю. Филатов
«10» ноября 2020 года

РЕГЛАМЕНТ (Порядок)
оказания услуг Удостоверяющего центра
АО «ПФ «СКБ Контур»

Екатеринбург
2020

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет регулирования

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://ca.kontur.ru.

1.1.3. Порядок распространяет свое действие на всех лиц, которые в силу настоящего Порядка, договора или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Порядком: Заявитель, Участники электронного взаимодействия, Владелец сертификата, Удостоверяющий центр (далее – Субъекты).

1.2. Присоединение к Порядку. Заключение договора на оказание услуг Удостоверяющего центра

1.2.1. Лицо, подавшее Заявление на выдачу Сертификата, присоединяется к настоящему Порядку, в том числе к публичному договору на оказание услуг Удостоверяющего центра, являющемуся неотъемлемой частью Порядка, в силу статьи 428 Гражданского кодекса Российской Федерации и обязано соблюдать его требования. Форма Заявления на выдачу Сертификата является Приложением № 11 к настоящему Порядку.

1.2.2. Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром в рамках Порядка, направив в Удостоверяющий центр Заявление на прекращение действия выданного ему Сертификата. Форма Заявления на прекращение действия Сертификата является Приложением № 4 к настоящему Порядку.

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 Субъектов о внесении изменений (дополнений) в Порядок осуществляется Удостоверяющим центром путем публикации на сайте по адресу: https://ca.kontur.ru.

1.3.3. Изменения (дополнения), вносимые Удостоверяющим центром в Порядок, кроме изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон по истечению 10 (Десяти) календарных дней с даты их публикации на сайте по адресу: https://ca.kontur.ru.

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

1.3.5. Неотъемлемой частью настоящего Порядка являются Профили сертификатов, которые являются Приложением № 6 и Приложением № 7 к настоящему Порядку. Удостоверяющий центр вносит изменения в Профили сертификатов путем публикации их обновленных версий по адресу https://ca.kontur.ru. Изменения в Профили сертификатов вступают в силу в порядке описанном в пункте 1.3.3 настоящего Порядка.

1.4. Сведения об Удостоверяющем центре

1.4.1. Удостоверяющий центр – организация, осуществляющая функции по созданию и выдаче сертификатов ключей проверки электронных подписей и иные функции удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

1.4.2. Акционерное общество «Производственная фирма «СКБ Контур» (ИНН 6663003127), именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Екатеринбурге. Свидетельство о регистрации № 0870-1 II-ОИ выдано 26.03.1996 администрацией Орджоникидзевского района г. Екатеринбурга.

1.4.3. 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 следующих документов:

– приказов Министерства связи и массовых коммуникаций от 06.08.2012 № 191, от 28.07.2017 № 389 «Об аккредитации удостоверяющих центров»;

– лицензии Управления Федеральной службы безопасности Российской Федерации по Свердловской области от 01.10.2020 рег. № 667 на бланке ЛСЗ 0008074 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 и индивидуального предпринимателя).

1.4.4. Юридический адрес и фактическое местонахождение Удостоверяющего центра: 620144, Екатеринбург, ул. Народной Воли, стр. 19А.

1.4.5. Адреса местонахождения обособленных подразделений (филиалов) Удостоверяющего центра указаны в Приложении № 9 к настоящему Порядку.

1.4.6. Удостоверяющий центр осуществляет свою работу в круглосуточном режиме. Информация о времени посещения офиса Удостоверяющего центра или обособленного подразделения (филиала) Удостоверяющего центра предоставляется при обращении Заявителя по контактным данным, указанным на официальном сайте Удостоверяющего центра: http://ca.kontur.ru.

1.5. Порядок информирования о предоставлении услуг Удостоверяющего центра

1.5.1. Информирование по вопросам предоставления услуг Удостоверяющего центра осуществляется следующими способами:

1) по контактному номеру телефона: тел.: 8-800-5000-508;
2) по адресу электронной почты: e-mail: ca@kontur.ru;
3) путем опубликования информации на официальном сайте: http://ca.kontur.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: http://ca.kontur.ru.

1.5.3. Адреса местонахождения, справочные телефоны, адреса электронной почты и официальных сайтов Доверенных лиц Удостоверяющего центра опубликованы на официальном сайте Удостоверяющего центра: http://ca.kontur.ru.

1.6. Стоимость услуг Удостоверяющего центра

1.6.1. Удостоверяющий центр осуществляет свою деятельность на платной основе.

1.6.2. Стоимость и состав услуг Удостоверяющего центра устанавливается Прайс-листом Удостоверяющего центра. Прайс-лист является Приложением № 8 к настоящему Порядку.

1.6.3. Информирование о стоимости услуг Удостоверяющего центра осуществляется путем публикации Порядка Удостоверяющего центра и приложений к нему в информационно-телекоммуникационной сети «Интернет» по адресу: http://ca.kontur.ru.

1.6.4. Сроки и порядок расчетов за оказание услуг Удостоверяющего центра устанавливается в Публичном договоре на оказание услуг Удостоверяющего центра. Публичный договор является Приложением № 1 к настоящему Порядку.

1.6.5. Сроки и порядок расчетов за оказание услуг Удостоверяющего центра могут быть изменены по согласованию с Заявителем.

1.6.6. В случае выполнения внеплановой смены Ключа электронной подписи Удостоверяющего центра Удостоверяющий центр безвозмездно создаёт Сертификаты для всех Владельцев сертификатов, чьи сертификаты прекращают действие в связи с внеплановой заменой.

1.6.7. Удостоверяющий центр в порядке, предусмотренном настоящим Порядком, безвозмездно предоставляет Сертификаты в форме электронных документов из Реестра сертификатов.

1.7. Термины и определения

1.7.1. Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

1.7.2. 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.

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

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

1.7.5. Неквалифицированная электронная подпись (далее − НЭП) – усиленная электронная подпись, соответствующая следующим признакам:

– получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи;

– позволяет определить лицо, подписавшее электронный документ;

– позволяет обнаружить факт внесения изменений в электронный документ после его подписания;

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

– получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ;

– позволяет определить лицо, подписавшее электронный документ;

– позволяет обнаружить факт внесения изменений в электронный документ после его подписания;

– ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

1.7.7. Сертификат ключа проверки электронной подписи (далее – Сертификат) – электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. По тексту настоящего Порядка употребление термина «Сертификат» означает как Сертификат НЭП, так и Сертификат КЭП.

1.7.8. Средство электронной подписи – шифровальное (криптографическое) средство, соответствующее следующим признакам:

– используется для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи;

– соответствует требованиям к средствам электронной подписи, утверждённым Приказом ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

1.7.9. Средство удостоверяющего центра – программное и (или) аппаратное средство, используемое Удостоверяющим центром для выполнения своих функций и соответствующее требованиям к средствам удостоверяющего центра, утверждённым Приказом ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

1.7.10. Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме органы государственной власти или органы местного самоуправления (далее – органы власти), индивидуальные предприниматели, юридические и физические лица.

1.7.11. 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.

1.7.12. Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее оператором или соглашением участников этой информационной системы.

1.7.13. Владелец сертификата ключа проверки электронной подписи (далее – Владелец сертификата) – лицо, которому в установленном настоящим Порядком порядке выдан сертификат ключа проверки электронной подписи, в соответствии с Федеральным законом № 63-ФЗ. Для Сертификата юридического лица вторым Владельцем является физическое лицо, данные о котором по заявлению юридического лица внесены в его Сертификат (Уполномоченный представитель Заявителя – юридического лица). В случаях, предусмотренных пунктом 3 статьи 14 Федерального закона № 63-ФЗ, данные о физическом лице в Сертификат не вносятся, единственным Владельцем сертификата является юридическое лицо.

1.7.14. Заявитель − юридическое лицо независимо от организационно-правовой формы, физическое лицо или иной хозяйствующий субъект (в том числе индивидуальный предприниматель, адвокат, нотариус и т.д.), обращающиеся в Удостоверяющий центр для получения Сертификата. После создания Сертификата Заявитель становится Владельцем сертификата.

1.7.15. Уполномоченный представитель Заявителя – юридического лица (Владельца сертификата) (далее – Уполномоченный представитель) – физическое лицо, которое действует от имени Заявителя (Владельца сертификата) – юридического лица или иного хозяйствующего субъекта на основании учредительных документов юридического лица или доверенности и которое указывается в Сертификате данного лица или субъекта в качестве второго Владельца наряду с наименованием первого Владельца сертификата – юридического лица, иного хозяйствующего субъекта.

1.7.16. Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по созданию электронных подписей под выдаваемыми Удостоверяющим центром Сертификатами в электронной форме и формируемыми Реестрами сертификатов, а также иными полномочиями согласно настоящему Порядку.

1.7.17. Доверенное лицо Удостоверяющего центра – действующее на основании договора с Удостоверяющим центром юридическое лицо или индивидуальный предприниматель, наделенные Удостоверяющим центром полномочиями по приему Заявлений на выдачу сертификатов ключей проверки электронной подписи (Приложение №11 к настоящему Регламенту), полномочиями по вручению ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром, а также иными полномочиями согласно настоящему Порядку.

1.7.18. Центр выдачи – обособленное подразделение (филиал) Удостоверяющего центра или Доверенное лицо Удостоверяющего центра.

1.7.19. Реестр сертификатов – реестр выданных и отозванных Удостоверяющим центром Сертификатов, включающий в себя информацию, содержащуюся в выданных этим Удостоверяющим центром Сертификатах, информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях такого прекращения и аннулирования.

1.7.20. Профиль Сертификата – документ, определяющий области применения, структуру и содержимое полей Сертификата, а также и перечень документов, необходимых для создания таких Сертификатов.

1.7.21. Ключевой носитель − физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации: Ключа ЭП, Ключа проверки ЭП и Сертификата.

1.7.22. Фотофиксация – осуществление фотосъемки будущего владельца Сертификата в анфас со страницей паспорта, на которой размещена фотография. Производится в целях сбора доказательственной базы исполнения Удостоверяющим центром требований Федерального закона № 63-ФЗ с помощью специально предназначенного для данных целей фотоаппарата.

1.7.23. Атака – проведение целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой информации или с целью создания условий для этого.

1.7.24. Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

2.1. Создание и выдача Сертификатов в электронной форме.
2.2. Изготовление заверенных копий Сертификатов на бумажном носителе по запросу.
2.3. Осуществление подтверждения владения заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному для получения Сертификата.
2.4. Установление сроков действия Сертификатов.
2.5. Аннулирует выданные Удостоверяющим центром Сертификаты по запросам Владельцев сертификатов и в иных случаях, установленных Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и Заявителем, а также настоящим Порядком. Услуги оказывается путём внесения сведений о прекращении действия в Реестр сертификатов.
2.6. Выдача Средств электронной подписи, обеспечивающих возможность создания Ключа ЭП и Ключа проверки ЭП.
2.7. Ведение Реестра сертификатов.
2.8. Установление порядка ведения реестра Сертификатов НЭП.
2.9. Создание Ключей проверки ЭП и Ключей ЭП с гарантией обеспечения конфиденциальности Ключей ЭП.
2.10. Проверка уникальности Ключей проверки ЭП в Реестре сертификатов.
2.11. Проверка действительности ЭП, Ключи проверки которых содержатся в Сертификатах, выданных Удостоверяющим центром, в Электронных документах.
2.12. Предоставление сведений об аннулированных Сертификатах и Сертификатах, действие которых прекращено, в том числе опубликование Реестра сертификатов по адресам, вносимым в соответствующее дополнение Сертификатов.
2.13. Выдача Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи, содержащего условия и порядок использования Сертификатов, ключей ЭП и средств ЭП. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи является Приложением № 12 к настоящему Порядку.
2.14. Информирование лиц, обращающихся в Удостоверяющий центр для выдачи Сертификата, о рисках, связанных с использованием ЭП.
2.15. Предоставление возможности Заявителю создать Ключи проверки ЭП и Ключи ЭП с гарантией обеспечения конфиденциальности Ключей ЭП в Центрах выдачи, имеющих необходимые лицензии ФСБ России на осуществление соответствующего вида деятельности.
2.16. Представление по запросу Участников электронного взаимодействия Сертификатов, внесённых в Реестр сертификатов Удостоверяющего центра, в форме электронных документов.
2.17. Удостоверяющий центр по отношению к Доверенным лицам является головным Удостоверяющим центром и реализует следующие функции:
2.17.1. осуществление проверки ЭП, Ключи проверки которых указаны в выданных Доверенными лицами Сертификатах;
2.17.2. обеспечение электронного взаимодействия Доверенных лиц между собой, а также Доверенных лиц с Удостоверяющим центром.
2.18. Выполнение иных функций, связанных с использованием ЭП, установленных действующим законодательством Российской Федерации.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА. ОТВЕТСВЕННОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. Права Удостоверяющего центра

3.1.1. 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.

3.1.2. Запросить фотоизображение будущего владельца Сертификата в анфас со страницей паспорта, на которой размещена фотография. В случае отказа предоставить фотоизображение (произвести фотофиксацию) Удостоверяющий центр вправе потребовать предоставить письменный отказ, выполненный будущим владельцем Сертификата. Письменный отказ в полном объеме должен быть выполнен собственноручно и должен содержать ссылку на факт отказа от предоставления фотоизображения (фотофиксации), а также фамилию, имя, отчество, дату и расшифровку подписи. Шаблон отказа от проведения фотофиксации является Приложением № 13 к настоящему 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 – физического лица и Уполномоченного представителя Заявителя – юридического лица с использованием технических средств.

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

3.1.6. Отказать в выдаче Сертификата в случае невыполнения обязанностей, указанных в подразделе 4.1 настоящего Порядка, а также в случае, если услуга по созданию и выдаче Сертификата не оплачена в надлежащем порядке.

3.1.7. Отказать в выдаче Сертификата в случае подачи Заявления на выдачу Сертификата с ошибками, исправлениями, подчистками и/или приписками, не подтвержденными собственноручной подписью Уполномоченного представителя Заявителя – юридического лица или Заявителя – физического лица.

3.1.8. Отказать в выдаче Сертификата в случае, если Заявитель-физическое лицо или Уполномоченный представитель Заявителя – юридического лица не предоставил письменного согласия на обработку своих персональных данных.

3.1.9. Отказать в выдаче Сертификата в случае, если не было подтверждено, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения Сертификата.

3.1.10. Отказать в выдаче Сертификата в случае, если Заявитель отказывается или уклоняется от посещения Удостоверяющего центра лично, когда это необходимо в целях подтверждения его волеизъявления, предоставленной информации и документов или удостоверения его личности.

3.1.11. Отказать в выдаче Сертификата в случае, если Заявитель – физическое лицо или Уполномоченный представитель Заявителя – юридического лица не согласился с обработкой и хранением персональных данных с помощью технических средств.

3.1.12. Отказать в прекращении действия Сертификата в случае ненадлежащего оформления Заявления на прекращение действия Сертификата, а также в случае, если Сертификат аннулирован или прекратил своё действие по другим основаниям.

3.1.13. Отказать в выдаче Сертификата в случае, если будущий владелец Сертификата не предоставил фотоизображение в анфас со страницей паспорта, на которой размещена фотография, или выполненный собственноручно отказ от предоставления фотоизображения (фотофиксации).

3.1.14. Без уведомления прекратить действие Сертификата в случае невыполнения Владельцем сертификата обязанностей, указанных в подразделе 4.3 настоящего Порядка, а также в

случае появления достоверных сведений о том, что документы, представленные в соответствии с подразделом 4.1 настоящего Порядка, не являются подлинными или не подтверждают достоверность всей информации, включённой в данный Сертификат, и/или в случае, если услуга по созданию и выдаче данного Сертификата не оплачена в надлежащем порядке.

3.1.15. Прекратить действие Сертификата в случае получения Удостоверяющим центром подтверждения факта смерти Владельца сертификата − физического лица, факта внесения в Единый государственный реестр юридических лиц записи о ликвидации Владельца сертификата-юридического лица, факта утраты силы государственной регистрации Владельца сертификата-физического лица в качестве индивидуального предпринимателя, главы крестьянского (фермерского) хозяйства, а также в случае вступления в силу судебного решения о дисквалификации Уполномоченного представителя Владельца сертификата – юридического лица.

3.1.16. Использовать представленные Заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия Сертификата, аутентификационной информации в соответствии с пунктом 6.2.1 настоящего Порядка и иной информации.

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

3.1.18. Удостоверяющий центр вправе наделить Доверенных лиц полномочиями по вручению Сертификатов от имени Удостоверяющего центра. При вручении Сертификата Доверенное лицо обязано установить личность получателя Сертификата (Заявителя) либо полномочия лица, выступающего от имени Заявителя – юридического лица, по обращению за получением данного Сертификата в соответствии с порядком реализации функций Удостоверяющего центра и исполнения его обязанностей, установленным наделившим указанное Доверенное лицо полномочиями по вручению Сертификатов Удостоверяющим центром с учетом предусмотренных пунктом 4 части 4 статьи 8 Федерального закона № 63-ФЗ требований. Удостоверяющий центр не вправе наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени Удостоверяющего центра.

3.2. Обязанности Удостоверяющего центра

3.2.1. Информировать в письменной форме заявителей об условиях и о прядке 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. Аккредитованный Удостоверяющий центр одновременно с выдачей квалифицированного Сертификата должен выдать владельцу квалифицированного Сертификата Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

3.2.2. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к Реестру сертификатов информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании Сертификата.

3.2.3. Обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.

3.2.4. Обеспечивать конфиденциальность фотоизображений будущего Владельца сертификата.

3.2.5. Отказать Заявителю в создании Сертификата в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения Сертификата.

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

3.2.7. Использовать для создания Сертификатов Средства Удостоверяющего центра, получившие подтверждение соответствия требованиям действующего законодательства.

3.2.8. Оказывать услуги в соответствии с требованиями, устанавливаемыми Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами.

3.2.9. С использованием инфраструктуры Единой системы межведомственного электронного взаимодействия (далее – СМЭВ) осуществлять с использованием государственных реестров проверку достоверности документов и сведений, представленных Заявителем.

3.2.10. Вносить в создаваемые Сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами и сведениями, полученными из государственных реестров.

3.2.11. При выдаче квалифицированного Сертификата аккредитованный Удостоверяющий центр обязан:

3.2.11.1. установить личность Заявителя – физического лица, обратившегося к нему за получением квалифицированного Сертификата;

3.2.11.2. получить от лица, выступающего от имени Заявителя – юридического лица, подтверждение правомочия обращаться за получением квалифицированного Сертификата.

3.2.12. При выдаче квалифицированного Сертификата аккредитованный Удостоверяющий центр направляет в Единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный Сертификат, в объеме, необходимом для регистрации в Единой системе идентификации и аутентификации, и о полученном им квалифицированном Сертификате (уникальный номер квалифицированного Сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного Удостоверяющего центра) в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ.

3.2.13. При выдаче квалифицированного Сертификата аккредитованный Удостоверяющий центр по желанию лица, которому выдан квалифицированный Сертификат, безвозмездно осуществляет регистрацию указанного лица в Единой системе идентификации и аутентификации.

3.2.14. В течение срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, хранить информацию о реквизитах основного документа, удостоверяющего личность Владельца сертификата – физического лица; о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени Заявителя – юридического лица, обращаться за получением Сертификата; о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца Сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях Владельца сертификата включена в Сертификат.

3.2.15. Для подписания от своего имени Сертификатов КЭП использовать квалифицированную электронную подпись, основанную на квалифицированном Сертификате, выданном головным удостоверяющим центром.

3.2.16. Обеспечивать круглосуточную доступность Реестра сертификатов в сети Интернет, за исключением периодов планового или внепланового технического обслуживания.

3.2.17. Осуществлять формирование и ведение Реестра сертификатов.

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

3.2.19. В случае принятия решения о прекращении своей деятельности аккредитованный Удостоверяющий центр обязан:

3.2.17.1. сообщить об этом в уполномоченный федеральный орган не позднее чем за 1 (Один) месяц до даты прекращения своей деятельности;

3.2.17.2. передать в уполномоченный федеральный орган в установленном порядке Реестр выданных этим аккредитованным Удостоверяющим центром квалифицированных Сертификатов;

3.2.17.3. передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном Удостоверяющем центре.

3.2.20. Предоставить Заявителю по его требованию копии документов, на основании которых осуществляет свою деятельность.

3.2.21. Произвести регистрацию Сертификата КЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ.

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

3.3. Ответственность Удостоверяющего центра

3.3.1. Удостоверяющий центр несет гражданско-правовую и (или) административную ответственность, а его работники несут гражданско-правовую и (или) 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 реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

3.3.2. Удостоверяющий центр в соответствии с законодательством Российской Федерации будет нести ответственность за вред, причиненный третьим лицам в результате:

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

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

3.3.3. Удостоверяющий центр не будет нести ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Порядку, а также возникшие в связи с этим убытки в случаях:

– если Удостоверяющий центр обоснованно полагался на сведения, представленные Заявителем;

– подделки, подлога либо иного искажения Заявителем, Владельцем сертификата либо третьими лицами информации, содержащейся в заявлении либо иных документах, представленных в Удостоверяющий центр.

3.3.4. Удостоверяющий центр не будет нести ответственность за невозможность использования Сертификата в случае, если такая невозможность возникла после создания Сертификата и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

4. ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СЕРТИФИКАТА

4.1. Обязанности Заявителя

4.1.1. Предъявить документы, удостоверяющие личность Уполномоченного представителя Заявителя – юридического лица, Заявителя – физического лица в соответствии с пунктом 6.2.4 настоящего Порядка.

4.1.2. Обеспечить личную явку в Центр выдачи Заявителя – физического лица или Уполномоченного представителя Заявителя – юридического лица.

4.1.3. Представить в Удостоверяющий центр документы, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем, и иные необходимые для создания Сертификата документы. Перечень документов, необходимых для создания Сертификата, определяется Профилем Сертификата с учетом положений пункта 3.1.1 настоящего Порядка.

4.1.4. По требованию Удостоверяющего центра обеспечить личную явку в Центр выдачи представителя Заявителя – юридического лица, данные о котором внесены в Единый государственный реестр юридических лиц (далее – ЕГРЮЛ) (лицо, имеющее право действовать без доверенности от имени юридического лица), а также совершить иные действия, направленные на обеспечение безопасности и законности процесса выдачи Сертификата (в том числе с использованием различных технических средств).

4.1.5. Не пересылать фотоизображение будущего Владельца сертификата в анфас с паспортом по незащищенным каналам связи.

4.1.6. По требованию Удостоверяющего центра загружать фотоизображение будущего Владельца сертификата в анфас со страницей паспорта, на которой размещена фотография, либо предоставлять в Удостоверяющий центр собственноручный письменный отказ.

В случае несогласия будущего Владельца сертификата предоставить фотоизображение в анфас со страницей паспорта, на которой размещена фотография, предоставить письменный собственноручно выполненный будущим Владельцем сертификата отказ.

4.2. Права Владельца сертификата

4.2.1. Обратиться в Удостоверяющий центр для прекращения действия выданного ему Сертификата в течение срока его действия.

4.2.2. Получить средства (средство) электронной подписи, получившие (получившее) 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).

4.2.3. Получить под расписку от Удостоверяющего центра инструкции по обеспечению безопасности использования электронной подписи и Средств электронной подписи.

4.2.4. Владелец Сертификата, выданного в форме электронного документа, вправе получить также копию Сертификата на бумажном носителе, заверенную Удостоверяющим центром.

4.3. Обязанности Владельца сертификата

4.3.1. Все обязанности, предусмотренные подразделом 5.2 настоящего Порядка.

4.3.2. Обеспечить выполнение Правил по обеспечению безопасности на рабочем месте, опубликованных на сайте http://ca.kontur.ru.

4.3.3. Обеспечивать конфиденциальность Ключей электронных подписей, в частности, не допускать использование принадлежащих им Ключей электронных подписей без их согласия.

4.3.4. Не использовать Ключ электронной подписи, Сертификат ключа проверки которой выдан Удостоверяющим центром, и немедленно обратиться в Удостоверяющий центр для прекращения действия этого Сертификата, при наличии оснований полагать, что конфиденциальность этого Ключа электронной подписи нарушена.

4.3.5. 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.

4.3.6. При вручении Сертификата под расписку ознакомиться с информацией, включаемой в Сертификат, подтвердив этот факт предоставлением расписки в бумажном или электронном виде в соответствии с пунктом 6.2.7 настоящего Порядка.

4.3.7. 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.

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 Сертификат, находящийся 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 электронной подписи осуществляется Заявителем самостоятельно либо на своем рабочем месте, либо в Центре выдачи.

Заявитель создает Ключ электронной подписи и Ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

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

Ключ электронной подписи и Ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона № 63-ФЗ создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также необходимость выполнения требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для Заявителя.

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.

Процедура плановой смены Ключей осуществляется в течение 1 (Одного) рабочего дня в следующем порядке:

1) Уполномоченное лицо Удостоверяющего центра формирует новый Ключ электронной подписи и соответствующий ему Ключ проверки электронной подписи;

2) В случае создания Удостоверяющим центром Ключа электронной подписи для подписания от своего имени неквалифицированных сертификатов, Уполномоченное лицо

Удостоверяющего центра изготавливает Сертификат и подписывает его созданным Ключом электронной подписи.

3) В случае создания Удостоверяющим центром Ключа электронной подписи для подписания от своего имени квалифицированных сертификатов, Уполномоченное лицо направляет соответствующее заявление и запрос на сертификат в головной удостоверяющий центр, функции которого осуществляет уполномоченный федеральный орган в порядке, предусмотренном Регламентом головного удостоверяющего центра. Головной удостоверяющий центр выдает квалифицированный сертификат и вручает его Удостоверяющему центру.

4) Старый Ключ электронной подписи (подвергшийся процедуре плановой смены) Удостоверяющего центра используется в течение своего срока действия для формирования перечня прекративших свое действие сертификатов из числа тех Сертификатов, которые были созданы в период действия старого Ключа электронной подписи.

5) Удостоверяющий центр информирует Владельцев сертификатов, которые прекращают свое действие, о факте плановой смены Ключей Удостоверяющего центра посредством размещения информации на официальном сайте Удостоверяющего центра: http://ca.kontur.ru. Для доверенного получения нового сертификата Удостоверяющего центра Владельцы сертификатов обращаются в Центры выдачи 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.

К угрозам нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра относятся угрозы, представляющие собой целенаправленные действия с использованием следующих возможностей:

– Подготовка и проведение атак из контролируемой зоны.

– Подготовка и проведение атак без использования доступа к функциональным возможностям программно-аппаратных средств взаимодействия с Удостоверяющим центром.

– Самостоятельное осуществление создания способов атак, подготовки и проведения атак на следующие объекты:

  – документацию на средства Удостоверяющего центра;

  – защищаемые электронные документы;

  – ключевую, аутентифицирующую и парольную информацию;

  – средства Удостоверяющего центра, их программные и аппаратные компоненты;

  – данные, передаваемые по каналам связи;

  – помещения, в которых находятся аппаратные средства, на которых реализованы средства Удостоверяющего центра, а также другие защищаемые ресурсы информационной системы.

– Внесение на этапах разработки, производства, хранения, транспортировки и ввода в эксплуатацию средств Удостоверяющего центра:

  – негативных функциональных возможностей в средства Удостоверяющего центра, в том числе с использованием вредоносных программ;

  – несанкционированных изменений в документацию на средства Удостоверяющего центра.

– Получение следующей информации:

  – общих сведений об информационной системе, в которой используются средства Удостоверяющего центра (назначение, состав, объекты, в которых размещены ресурсы информационной системы);

  – сведений об информационных технологиях, базах данных, автоматизированной системы, программном обеспечении, используемых в информационной системе совместно со средствами Удостоверяющего центра;

  – сведений о физических мерах защиты объектов, в которых размещены средства Удостоверяющего центра;

- сведений о мерах по обеспечению защиты контролируемой зоны объектов информационной системы, в которой используются средства Удостоверяющего центра;
- сведений о мерах по разграничению доступа в помещения, в которых размещены средства Удостоверяющего центра;
- содержания находящейся в свободном доступе технической документации на средства Удостоверяющего центра;
- сведений о защищаемой информации, используемой в процессе эксплуатации средств Удостоверяющего центра (виды защищаемой информации: служебная информация, парольная и аутентифицирующая информация, конфигурационная информация, управляющая информация, информация в электронных журналах регистрации; общие сведения о содержании каждого вида защищаемой информации; характеристики безопасности для каждого вида защищаемой информации);
- всех возможных данных, передаваемых в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационно-техническими мерами;
- сведений о линиях связи, по которым передается защищаемая с использованием средств Удостоверяющего центра информация;
- сведений обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами, нарушениях правил эксплуатации средств Удостоверяющего центра;
- сведений обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами, неисправностях и сбоях средств Удостоверяющего центра;
- сведений, получаемых в результате анализа любых доступных для перехвата сигналов от аппаратных компонентов средств Удостоверяющего центра.

– Использование:
  - находящихся в свободном доступе или за пределами контролируемой зоны автоматизированной системы и программного обеспечения, включая программные и аппаратные компоненты средств Удостоверяющего центра;
  - специально разработанных автоматизированных систем и программного обеспечения.

– Использование в качестве каналов атак не защищенных от несанкционированного доступа к информации организационно-техническими мерами каналов связи (как вне контролируемой зоны, так и в ее пределах), по которым передается информация, обрабатываемая средствами Удостоверяющего центра.

– Подготовка и проведение атак без использования доступа к автоматизированной системе, на которых реализованы средства Удостоверяющего центра.

– Использование штатных средств информационной системы, в которой используются средства Удостоверяющего центра.

Для нейтрализации угроз нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра реализован изолированным режим работы программно-аппаратного комплекса Удостоверяющего центра − комплекс организационно-технических мер, при выполнении которых нарушитель не располагает программно-аппаратными средствами взаимодействия с Удостоверяющим центром.

К случаям нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра относятся события, включая, но не ограничиваясь:

– 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) закрытого ключа.

– 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).

Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых Ключ электронной подписи Удостоверяющего центра может стать доступными несанкционированным лицам и (или) процессам, является основанием полагать, что конфиденциальность такого Ключа электронной подписи нарушена.

В случае нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра или угрозы нарушения конфиденциальности такого Ключа электронной подписи выполняется внеплановая смена соответствующего Ключа.

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

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 старым 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 на электронную почту, указанную в сертификате и размещения информации на официальном сайте Удостоверяющего центра: http://ca.kontur.ru.

В целях исключения возможности уничтожения, модифицирования, блокирования при передаче и иных неправомерных действий с квалифицированным сертификатом, Владельцы Сертификатов могут доверенным способом получить новый Сертификат Удостоверяющего центра в Центре выдачи.

После получения уведомления о факте внеплановой смены Ключей Удостоверяющего центра Владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых Сертификатов в соответствии с порядком, установленным подразделом 6.2 настоящего Порядка.

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

Смена ключа электронной подписи владельца Сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи Федерального закона № 63-ФЗ.

Заявление на смену ключа электронной подписи составляется по форме, установленной Приложением № 14 к настоящему порядку.

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

Процедура выдачи Сертификата и ключа электронной подписи (при необходимости) 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.

Заявитель обращается за выдачей Сертификата в Центр выдачи. В Центре выдачи производится формирование Заявления на выдачу Сертификата, принимаются представленные Заявителем документы, вручаются готовые Сертификаты. В отдельных случаях, устанавливаемых Профилем Сертификата, Центр выдачи может предоставить Заявителю доступ к автоматизированной корпоративной информационной системе «Кабинет УЦ» (далее – АС «Кабинет 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 Центре выдачи.

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

Будущий владелец Сертификата осуществляет фотосъемку в анфас со страницей паспорта, на которой размещена фотография, и размещает фотоизображение через Личный кабинет в АС «Кабинет УЦ». В случае отказа от предоставления фотоизображения будущий владелец Сертификата предоставляет письменный отказ.

6.2.2. Требование к заявлению на создание и выдачу Сертификатов.

Заявление подается по форме, утвержденной Удостоверяющим центром. Заявление на выдачу Сертификата может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручно, так и в электронном виде, подписанное КЭП. С примерами заявлений на выдачу Сертификата можно ознакомиться по адресу http://ca.kontur.ru. Данные примеры носят исключительно ознакомительный характер, за получением актуальных форм заявлений на выдачу Сертификата Заявитель обращается в Центр выдачи (адреса Центров выдачи публикуются на сайте http://ca.kontur.ru). Актуальную форму Заявления на выдачу Сертификата Удостоверяющий центр определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия. Собственноручное подписание Заявления на бумажном носителе производится чернилами (пастой) синего цвета. Использование факсимиле (клише подписи) на Заявлении на выдачу Сертификата не допускается.

Удостоверяющий центр принимает заявление в электронном виде, если заявление Заявитель подписывает действующим Сертификатом, выданным удостоверяющим центром, аккредитованным в соответствии с Федеральным законом № 63-ФЗ.

6.2.3. Порядок установления личности.

Личность Заявителя − физического лица и Уполномоченного представителя Заявителя – юридического лица устанавливается двумя способами:

6.2.3.1. При личном обращении при предъявлении следующих документов:

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспорту гражданина Российской Федерации . В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, признаваемому таковым действующим законодательством.

Личность гражданина иностранного государства устанавливается 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.

Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, признаваемого действующим законодательством в качестве удостоверяющего личность данных категорий лиц.

6.2.3.2. При подаче заявления, подписанного квалифицированной электронной подписью, сертификат ключа проверки которой принадлежит лицу, личность которого устанавливается,

который выдан удостоверяющим центром, аккредитованным в соответствии с Федеральным законом № 63-ФЗ.

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

Перечень документов и сведений, запрашиваемых Удостоверяющим центром у Заявителя, необходимых для изготовления и выдачи Сертификата, в том числе для удостоверения личности Заявителя, устанавливается в соответствии с частью 2 статьи 17 и частью 2 статьи 18 Федерального закона № 63-ФЗ.

Удостоверяющий центр выполняет свою обязанность по внесению в Сертификат только достоверной и актуальной информации путем сбора и хранения сканкопий документов, представленных Заявителем, а также путем запроса соответствующих сведений из государственных реестров

Заявитель представляет в Удостоверяющий центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения Уполномоченного представителя Заявителя – юридического лица, Заявителя – физического лица, а также документы, на основании которых Удостоверяющим центром вносятся сведения в Сертификат, такие как: полное или сокращенное наименование, основной государственный регистрационный номер, юридический адрес, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, наименование должности и иные данные.

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

При обращении в Удостоверяющий центр Уполномоченного представителя Заявителя – юридического лица его полномочия должны быть подтверждены данными в ЕГРЮЛ (лицо, имеющее право действовать без доверенности от имени юридического лица), для любого иного уполномоченного лица, данные о котором вносятся в Сертификат, полномочия должны быть подтверждены соответствующей доверенностью.

Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти (например, налоговыми органами), заверение копий документов Заявителем самостоятельно. При необходимости копии с документов могут быть сняты и заверены сотрудником Удостоверяющего центра или Центра выдачи. Допустимые способы заверения копий документов описаны в Профиле Сертификата.

Нотариально заверенные копии документов должны содержать штамп нотариуса «копия верна», штамп с информацией о нотариусе, должны быть заверены печатью нотариуса и иметь подпись нотариуса.

Копии, заверенные Заявителем, могут предоставлять исключительно юридические лица и индивидуальные предприниматели, имеющие собственную печать. Многостраничные копии либо должны быть прошиты и заверены на листе сшивки, либо на каждой странице такой копии должна иметься отдельная заверительная надпись. Образец заверительной надписи:

ВЕРНО Должность с указанием наименования организации/индивидуального предпринимателя Подпись Расшифровка подписи (фамилия и инициалы полностью) Дата заверения документа Оттиск печати

Копии документов, заверенные органом власти, должны содержать подпись и расшифровку подписи должностного лица, их заверившего, а также печать/штамп данного органа власти.

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

6.2.5. Порядок проверки достоверности документов и сведений, предоставленных заявителем.

Для заполнения Сертификата в соответствии с частью 2 статьи 17 Федерального закона № 63-ФЗ Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона № 63-ФЗ. В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в Сертификат, и Удостоверяющим центром установлена личность Заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени Заявителя – юридического лица, обращение за получением Сертификата, 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. Если Владельцем сертификата является юридическое лицо, то наряду с наименованием такого юридического лица в Сертификат может вноситься информация об Уполномоченном представителе. 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.

Особенности установления достоверности документов и сведений, представленных Заявителем для выдачи Сертификата, устанавливаются соответствующим Профилем Сертификата.

В случае внесения в Сертификат персональных данных физического лица, Заявитель – физическое лицо или Уполномоченный представитель Заявителя – юридического лица предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в Заявление на выдачу Сертификата. Персональные данные, внесенные в Сертификат, становятся общедоступными в соответствии с Федеральным законом № 63-ФЗ. Согласие должно быть подписано собственноручно лицом, данные о котором вносятся в Сертификат (субъектом персональных данных). Также согласие на обработку персональных данных может быть подписано представителем субъекта персональных данных, действующим на основании нотариальной доверенности, которая должна быть выдана от имени субъекта персональных данных, должна содержать полномочие на предоставление согласия на обработку персональных данных от имени субъекта персональных данных, а также должна соответствовать иным требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

Требования к структуре Сертификатов НЭП установлены в соответствующем Профиле Сертификата.

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

6.2.7. Порядок выдачи Сертификата.

При получении Сертификата Заявителем он должен быть ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в Сертификате. Подтверждение ознакомления с информацией, содержащейся в Сертификате, осуществляется под расписку в соответствии с частью 3 статьи 18 Федерального закона № 63-ФЗ.

Расписку на бумажном носителе, содержащую описание информации, включенной в Сертификат, Заявитель передает в Удостоверяющий центр при вручении Сертификата.

Факт создания Ключа электронной подписи и соответствующего ему Ключа проверки электронной подписи, содержащегося в Сертификате, Удостоверяющим центром, или факт создания данных Ключей Заявителем самостоятельно при помощи Средств электронной подписи, выданных ему Удостоверяющим центром, подтверждает факт владения Владельцем сертификата Ключом электронной подписи, соответствующим Ключу проверки электронной подписи, указанному в таком Сертификате. Каких-либо иных подтверждений владения Участники электронного взаимодействия не оформляют.

Информация, содержащаяся в Сертификате ключа проверки электронной подписи указана в Расписке, форма которой установлена Приложением № 10 к настоящему Порядку

6.2.8. Срок создания и выдачи Сертификата. Условия для срочного создания и выдачи Сертификата.

Создание Сертификата производится в течение трех рабочих дней с момента подачи Заявления на выдачу Сертификата, при условии подтверждения всех фактов соответствия сведений в Заявлении на выдачу Сертификата согласно пункту 6.2.6 настоящего Порядка.

Срочное создание и выдача Сертификата производится в соответствии с условиями прайс-листа Удостоверяющего центра.

6.3. Подтверждение действительности электронной подписи, использованной 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 на основании заявления на подтверждение действительности ЭП, форма которого установлена Приложением № 3 к настоящему Порядку.

К заявлению прикладывается электронный документ и ЭП, подтверждение которой производится.

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 услуг.

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 ЭП каждого сертификата, путем построения цепочки сертификатов до сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром;

– проверка действительности сертификатов на текущий момент времени;

– проверка отсутствия сертификатов в списках отозванных сертификатов (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 про-

изводится 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 Федеральным законом № 63-ФЗ.

Сертификат прекращает свое действие:

– по истечении срока его действия;

– по заявлению Владельца сертификата о прекращении действия Сертификата. Форма такого заявления приведена в Приложении № 4 к настоящему Порядку. Также заявление о прекращении действия ранее выданного Сертификата может содержаться в составе Заявления на выдачу Сертификата;

– в случае увольнения работника Удостоверяющего центра, которому был выдан Сертификат для выполнения трудовых обязанностей;

– по решению Удостоверяющего центра в случаях, предусмотренных пунктами 3.1.14, 3.1.15 настоящего Порядка;

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

– в случаях, установленных статьей 14 Федерального закона № 63-ФЗ.

Удостоверяющий центр аннулирует Сертификат, если:

– 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 (аннулировании) Сертификата.

Сотрудник Удостоверяющего центра или Центра выдачи при приеме заявления на прекращение действия Сертификата получает от Владельца сертификата подтверждение правомочия обращаться за прекращением действия Сертификата. Приём заявлений осуществляется в Центрах выдачи в рабочие дни в рабочее время (не ранее 8:00 и не позднее 19:00 местного времени).

Заявление подается по форме, утвержденной Удостоверяющим центром и установлена Приложением № 4 к настоящему Порядку. Заявление на прекращение действия Сертификата может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручно, так и в электронном виде, подписанное КЭП.

Информация о прекращении действия или аннулировании Сертификата вносится в Реестр сертификатов. Действие Сертификата прекращается с момента публикации Реестра сертификатов, в который внесён этот Сертификат. Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификата составляет не более 12 (двенадцати) часов с момента приема Заявления на прекращение действия Сертификата или наступления иного события, предусмотренного пунктом 6.4.1 настоящего Порядка. Более короткий срок может устанавливаться в Профиле сертификата.

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.

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 прекративших свое действие (аннулированных) Сертификатов 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 пунктом 6.4.1 настоящего Порядка. Более короткий срок может устанавливаться в Профиле сертификата.

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 производится посредством размещения информации на официальном сайте Удостоверяющего центра: http://ca.kontur.ru.

6.7. Подтверждение действительности ЭП Удостоверяющего центра в выданных Сертификатах.

Подтверждение действительности ЭП Удостоверяющего центра осуществляется на основании заявления, форма которого установлена Приложением № 2 к настоящему Порядку.

Срок проведения экспертизы составляет 15 (Пятнадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

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 выдается Заявителю одновременно с выдачей Сертификата, а также путем размещения Правил по обеспечению информационной безопасности на рабочем месте на официальном сайте УЦ: http://ca.kontur.ru.

7.2. Выдача по обращению заявителя средств электронной подписи.

Выдаваемые средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона «Об электронной подписи» 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.

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

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

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

– предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременным обнаружением фактов несанкционированного доступа к информации;

– 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 сертификатов.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к Реестру сертификатов, через форму запроса на официальном сайте Удостоверяющего центра: http://ca.kontur.ru, 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 Заявителем на автоматизированном рабочем месте, аттестованном на соответствие требованиям по безопасности информации, размещенном в помещении Центра выдачи, 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.

В случае нарушения конфиденциальности Ключа электронной подписи, а также в случаях наличия оснований полагать, что конфиденциальность Ключа электронной подписи была нарушена, Владелец сертификата Ключа проверки электронной подписи, соответствующего такому Ключу электронной подписи, должен прекратить использование этого Ключа и подать в Удостоверяющий центр Заявление на прекращение действия этого Сертификата.

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 Владельце Сертификата 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 Владельца Сертификата в ЕСИА.

7.8. Предоставление доступа к Реестру сертификатов.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к реестру квалифицированных сертификатов, с использованием специализированного онлайн-сервиса (далее – Сервис доступа). Обращение к Сервису доступа осуществляется по адресу https://ca.kontur.ru/about/reestr. Для получения доступа к Реестру выданных сертификатов заинтересованное лицо заполняет размещенную в Сервисе доступа форму запроса. Обработка запроса осуществляется в онлайн-режиме. Информация предоставляется заинтересованному лицу в форме электронного сообщения, формируемого в Сервисе доступа

8. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ И СЕРТИФИКАТОВ

8.1. Срок действия Ключей электронной подписи Удостоверяющего центра составляет не более 3 (Трех) лет. Начало периода действия Ключей электронной подписи Удостоверяющего центра исчисляется с момента начала действия его Сертификата.

8.2. Срок действия Сертификата Удостоверяющего центра составляет не более 15 (Пятнадцати) лет.

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

8.4. Срок действия Сертификата, создаваемого Удостоверяющим центром для Заявителя, равен сроку действия Ключа электронной подписи, соответствующего данному Сертификату.