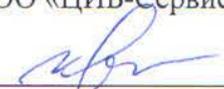


УТВЕРЖДАЮ
Директор
ООО «ЦИБ-Сервис»


Т. В. Красикова
«01» марта 2022 года

**Регламент (Порядок)
оказания услуг Удостоверяющего центра
ООО «ЦИБ-Сервис»**

Барнаул
2022

СОДЕРЖАНИЕ

1	Общие положения	3
2	Перечень реализуемых Удостоверяющим центром функций	7
3	Права и обязанности Удостоверяющего центра. Ответственность Удостоверяющего центра	8
4	Права и обязанности заявителя и Владельца Сертификата	11
5	Права и обязанности участников электронного взаимодействия	12
6	Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром	13
	6.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей	13
	6.2. Процедура создания и выдачи Сертификатов	15
	6.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов	18
	6.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата	18
	6.5. Порядок ведения Реестра сертификатов	19
	6.6. Порядок технического обслуживания Реестра сертификатов	20
	6.7. Подтверждение действительности электронной подписи удостоверяющего центра в выданных сертификатах	20
7	Порядок исполнения обязанностей Удостоверяющего центра	21
8	Сроки действия ключей и Сертификатов	23
	Приложение № 1. Публичный договор № 1/2021 на оказание услуг Удостоверяющего центра	
	Приложение № 2. Форма заявления на подтверждение электронной подписи Удостоверяющего центра в Сертификате	
	Приложение № 3. Форма заявления на подтверждение электронной подписи в электронном документе	
	Приложение № 4. Форма заявления на прекращение действия Сертификата	
	Приложение № 5. Форма заявления на смену абонентского номера подвижной (мобильной) связи	
	Приложение № 6. Профиль Сертификата	

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.

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.

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 Порядка являются Профиль Сертификатов. Удостоверяющий центр вносит изменения в Профиль сертификата путем публикации их обновленных версий по адресу <https://ca.kontur.ru>. Изменения в Профиль Сертификата вступают в силу в порядке пункта 1.3.3 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. Общество с ограниченной ответственностью «ЦИБ-Сервис», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Барнауле. Свидетельство о регистрации № 22 003555502 выдано 24.08.2011 Межрайонной инспекцией Федеральной налоговой службы России № 15 по Алтайскому краю, 2221.

1.4.3. Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании следующих документов:

– Приказа ООО «ЦИБ-Сервис» от 28.02.2022 № 2 «О возобновлении УЦ»;

– лицензии Управления Федеральной службы безопасности Российской Федерации по Алтайскому краю от 28.05.2018 рег. № 200 на бланке ЛСЗ 0011388 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, фактический адрес Удостоверяющего центра: 656031, Алтайский край, г. Барнаул, проспект Строителей, д. 117, пом. 60.

1.4.5. Удостоверяющий центр осуществляет свою работу в круглосуточном режиме. Информация о времени посещения офиса Удостоверяющего центра предоставляется при обращении Заявителя по контактными данным, указанным на официальном сайте Удостоверяющего центра <https://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: 8-800-5000-508;
- 2) по адресу электронной почты: ca@kontur.ru;
- 3) путем опубликования информации на официальном сайте: <https://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 <https://ca.kontur.ru>.

1.5.3. Адреса местонахождения, справочные телефоны, адреса электронной почты и официальных сайтов Центров выдачи Удостоверяющего центра опубликованы на официальном сайте Удостоверяющего центра <https://ca.kontur.ru>.

1.6. Стоимость услуг Удостоверяющего центра

1.6.1. Удостоверяющий центр осуществляет свою деятельность на платной основе.

1.6.2. 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.

1.6.3. 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. Простая электронная подпись (далее – ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Для создания ПЭП используется ключ ПЭП – сочетание идентификатора и пароля (кода). Допустимые форматы ключа ПЭП, а также случаи и порядок использования ПЭП определяются настоящим Порядком.

1.7.6. 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;

1.7.7. 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.

1.7.8. Неквалифицированный сертификат ключа проверки электронной подписи (далее – 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.

1.7.9. 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».

1.7.10. 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».

1.7.11. 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.

1.7.12. 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.

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

1.7.14. 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).

1.7.15. 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.

1.7.16. 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.

1.7.17. 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 Порядку.

1.7.18. Доверенное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра или Центра выдачи и наделенное Удостоверяющим центром полномочиями по вручению ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром, а также иными полномочиями согласно Порядку.

1.7.19. Центр выдачи – обособленное подразделение (филиал) Удостоверяющего центра или действующее на основании договора с Удостоверяющим центром юридическое лицо или индивидуальный предприниматель, и из числа сотрудников которого назначается Доверенное лицо Удостоверяющего центра.

1.7.20. 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.

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

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

1.7.23. 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.

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 электронной подписи, соответствующим ключу проверки электронной подписи, указанному для получения Сертификата.
- 2.4.** Установление сроков действия Сертификатов.
- 2.5.** Прекращение действия Сертификатов 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 оказываются путём внесения сведений о прекращении действия в Реестр сертификатов.
- 2.6.** Выдача Средств электронной подписи, обеспечивающих возможность создания Ключа электронной подписи и Ключа проверки.
- 2.7.** Ведение реестра Сертификатов.
- 2.8.** Установление порядка ведения реестра Сертификатов.
- 2.9.** Создание Ключей проверки и Ключей электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи.
- 2.10.** Проверка уникальности Ключей проверки 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 инструкций по информационной безопасности, содержащих условия и порядок использования сертификатов ЭП, Ключей ЭП и Средств ЭП.
- 2.14.** Информирование лиц, обращающихся в Удостоверяющий центр для выдачи Сертификата, о рисках, связанных с использованием ЭП.
- 2.15.** Представление по запросу Участников электронного взаимодействия Сертификатов, внесённых в Реестр сертификатов Удостоверяющего центра, в форме электронных документов.
- 2.16.** Выполнение иных функций, установленных действующим законодательством Российской Федерации.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА. ОТВЕТСТВЕННОСТЬ 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.

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 Порядка и Профиля Сертификата.

3.1.6. Отказать в выдаче Сертификата в случае невыполнения обязанностей, указанных в подразделе 4.1 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 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 Владелец сертификата обязанностей, указанных в подразделе 4.3 Порядка, а также в случае появ-

ления достоверных сведений о том, что документы, представленные в соответствии с подразделом 4.1 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 подразделом 6.2.1 Порядка и иной информации.

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

3.2. Обязанности Удостоверяющего центра

3.2.1. 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.

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

3.2.10. При выдаче Сертификата идентифицировать Заявителя – физического лица, обратившегося за получением Сертификата или личность и полномочия обращаться за получением Сертификата Уполномоченного представителя Заявителя – юридического лица способами, установленными пунктом 6.2.3. Порядка.

3.2.11. 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.

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

3.2.13. Осуществлять формирование и ведение Реестра сертификатов.

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

3.2.15. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр уведомляет о данном факте Владельцев сертификата, передает или уничтожает информацию, внесенную в реестр сертификатов в порядке, установленном пунктом 6 статьи 13 Федерального закона № 63-ФЗ.

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

3.2.17. 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 ответственность в соответствии с законодательством Российской Федерации.

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. Обеспечить возможность произведения идентификации Заявителя – физического лица или Уполномоченного представителя Заявителя – юридического лица, способами, предусмотренными п. 6.2.3. Порядка.

4.1.2. 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 Порядка.

4.1.3. По требованию Удостоверяющего центра обеспечить личную явку в Центр выдачи представителя Заявителя – юридического лица, данные о котором внесены в 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).

4.2. Права Владельца сертификата

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

4.2.2. На платной основе 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 от Удостоверяющего центра инструкции по обеспечению безопасности использования электронной подписи и Средств электронной подписи.

4.3. Обязанности Владельца сертификата

4.3.1. Все обязанности, предусмотренные подразделом 5.2 Порядка.

4.3.2. Обеспечить выполнение Правил по обеспечению безопасности на рабочем месте, опубликованных на сайте <https://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. В случае самостоятельного создания Ключа электронной подписи предоставить в Удостоверяющий центр запрос на выдачу сертификата в виде структуры CertificationRequest, определенной в пункте 7 Формата электронной подписи, утвержденного приказом Минцифры России от 14 сентября 2020 г. № 472, 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 используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи. При создании Ключа ЭП и запроса на Сертификат должен использоваться алгоритм ГОСТ Р 34.10-2012 с длиной ключа 256 бит.

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 неквалифицированной электронной подписи создаются с использованием средства электронной подписи, соответствующего требованиям Федерального закона № 63-ФЗ.

Создание Ключей электронной подписи осуществляется Заявителем самостоятельно на своем рабочем месте с использованием приобретенных в Удостоверяющем центре, либо собственных Средств электронной подписи.

В Удостоверяющем центре Ключ электронной подписи создается Заявителем – физическим лицом или Уполномоченным представителем Заявителя – юридического лица на автоматизированном рабочем месте, аттестованном на соответствие требованиям, установленным постановлением Правительства Российской Федерации от 3 февраля 2012 г. №79, размещенном в помещении Центра выдачи, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель.

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) При создании 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) 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.
- 4) 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.

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 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.

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

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

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

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) 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).

В случае компрометации или угрозы компрометации Ключа электронной подписи Удостоверяющего центра выполняется внеплановая смена соответствующего Ключа.

Процедура внеплановой смены Ключей Удостоверяющего центра выполняется в срок и в порядке, определенном процедурой плановой смены таких Ключей, согласно подразделу 6.1.2 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: <https://ca.kontur.ru>.

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

Владельцы Сертификатов могут доверенным способом получить новый Сертификат Удостоверяющего центра в Центре выдачи.

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

Смена ключа электронной подписи владельца Сертификата осуществляется в случаях, установленных действующим законодательством Российской Федерации.

Заявление на смену ключа электронной подписи составляется по форме, установленной Удостоверяющим центром. Образец заявления публикуется на сайте <https://ca.kontur.ru>.

Заявление на смену ключа электронной подписи владельца Сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца Сертификата.

Процедура выдачи Сертификата и ключа электронной подписи (при необходимости) осуществляется в соответствии с действующим законодательством Российской Федерации и настоящим Порядком.

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. 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.

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

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 <https://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 <https://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.

6.2.3. Порядок идентификации Заявителя.

Идентификация Заявителя проводится следующими способами:

- при личном обращении Заявителя при предъявлении документов, указанных в пунктах 2.4. и 3.3. Профиля сертификата;
- при подаче заявления на выдачу Сертификата, подписанного КЭП, сертификат ключа проверки которой принадлежит лицу, личность которого устанавливается, который выдан удостоверяющим центром, аккредитованным в соответствии с Федеральным законом № 63-ФЗ;
- без личного присутствия с использованием ПЭП, ключ которой получен при личной явке в соответствии с правилами использования ПЭП при обращении за получением

государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации, полученной посредством обращения к единой системе идентификации и аутентификации;

– при личном присутствии у нотариуса (в т.ч. должностные лица местного самоуправления, указанные в ч. 4 ст. 1 Основ законодательства Российской Федерации о нотариате, а также должностные лица консульских учреждений РФ) при подписании Заявления на выдачу сертификата. Нотариус удостоверяет личность Заявителя и заверяет его подпись на указанном заявлении. Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспорту гражданина РФ. В исключительных случаях отсутствия у гражданина РФ 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.

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

Перечень документов и сведений, необходимых для изготовления и выдачи Сертификата устанавливается действующим законодательством Российской Федерации об электронной подписи, а также в Профиле Сертификата (Приложение № 6 к Порядку).

Удостоверяющий центр вносит в Сертификат только достоверную и актуальную информацию на основании Заявления на выдачу сертификата. Ответственность за предоставленные сведения и документы несет Заявитель.

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 Заявления на выдачу сертификата могут являться копии, заверенные нотариусом, в т.ч. должностным лицом местного самоуправления, указанным в ч. 4 ст. 1 Основ законодательства Российской Федерации о нотариате, а также должностным лицом консульских учреждений РФ.

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

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом должностным лицом консульских учреждений РФ

6.2.5. 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 инфор-

мация 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).

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

В целях получения доказательств того, что заявитель владеет Ключом ЭП, который соответствует Ключу проверки ЭП, указанному заявителем для получения сертификата, Удостоверяющий центр руководствуется правилами, утвержденными приказом Федеральной службы безопасности Российской Федерации от 20.04.2021 № 154.

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

6.2.6. Порядок выдачи Сертификата.

По окончании процедуры создания Сертификата Удостоверяющий центр знакомит Заявителя с информацией, внесенной в Сертификат, и выдает Заявителю:

- Ключ электронной подписи и Сертификат (с ключом проверки ЭП)
- копию Сертификата на бумажном носителе (по запросу).

Заявителю предоставляется возможность ознакомиться с информацией, вносимой в Сертификат, в электронном виде, для подтверждения ознакомления с данной информацией Владелец сертификата подписывает ее ПЭП.

Заключением соглашения об использовании ПЭП является присоединение Заявителя к Порядку. Ключом ПЭП в АС «Кабинет УЦ» является сочетание номера подвижной (мобильной) связи, представленного Заявителем, и уникального случайно генерируемого кода аутентификации, отправленного Удостоверяющим центром на данный номер в форме SMS-сообщения. Введение Заявителем такого кода подтверждения позволяет Удостоверяющему центру определить лицо, поставившее ПЭП.

Заявитель обязан хранить в тайне ключ ПЭП, принимать все возможные меры, предотвращающие нарушение его конфиденциальности. В случае нарушения конфиденциальности ключа ПЭП Заявитель обязан незамедлительно уведомить об этом Удостоверяющий центр.

Информация в электронной форме, подписанная ПЭП в АС «Кабинет УЦ», признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

6.2.7. Срок 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 подразделу 6.2.4 Порядка.

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 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 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 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 Порядку;
- в случае увольнения работника Удостоверяющего центра и/или работника Группы компаний СКБ Контур, которому был выдан Сертификат для выполнения трудовых обязанностей;
- по решению Удостоверяющего центра в случаях, предусмотренных пунктами 3.1.14, 3.1.15 Порядка;

- в случае прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам.

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.

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

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 подразделом 6.4.1 Порядка.

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 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: <https://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 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 <https://ca.kontur.ru>.

7.2. Выдача по обращению заявителя средств электронной подписи.

Выдаваемые на платной основе 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: <https://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.

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. 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>, а также на основании официального мотивированного запроса с указанием причины обращения. 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 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.