



Приложение к приказу ООО ИК «СИБИНТЕК»  
от 14 08 2024 г. № 14-БА-00348-17

УТВЕРЖДЕНО

Генеральный директор

[Redacted signature box]

Ю.А. Попов

# Порядок реализации функций аккредитованного удостоверяющего центра ООО ИК «СИБИНТЕК» и исполнения его обязанностей

ВЕРСИЯ 3

г. Москва

2024 г.

## Оглавление

Термины и определения.....	4
1 Общие положения.....	6
1.1 Предмет регулирования Порядка.....	6
1.2 Сведения об Удостоверяющем центре.....	7
1.3 Порядок информирования о предоставлении услуг Удостоверяющего центра.....	7
1.4 Стоимость услуг Удостоверяющего центра.....	8
2 Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг).....	8
3 Права и обязанности Удостоверяющего центра.....	10
3.1 Права Удостоверяющего центра.....	10
3.2 Обязанности Удостоверяющего центра.....	10
3.3 Права Владельца сертификата.....	13
3.4 Обязанности Владельцев квалифицированного сертификата.....	14
3.5 Права Заявителя.....	14
3.6 Обязанности Заявителя.....	14
4 Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром.....	14
4.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей.....	14
4.1.1 Порядок создания ключей электронных подписей и ключей проверки электронных подписей.....	14
4.1.2 Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены.....	15
4.1.3 Информирование о смене ключей электронной подписи Удостоверяющего центра.....	16
4.1.4 Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Владельца квалифицированного сертификата.....	17
4.2 Процедура создания и выдачи квалифицированных сертификатов.....	17
4.2.1 Порядок подачи заявления на создание и выдачу квалифицированных сертификатов....	17
4.2.2 Требования к заявлению на создание и выдачу квалифицированных сертификатов.....	17
4.2.3 Порядок идентификации Заявителя (установления личности).....	18
4.2.4 Перечень документов, запрашиваемых Удостоверяющим центром у Заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности Заявителя.....	19
4.2.5 Порядок проверки достоверности документов и сведений.....	19
4.2.6 Порядок создания квалифицированного сертификата.....	20
4.2.7 Порядок выдачи квалифицированного сертификата.....	20
4.2.8 Срок создания и выдачи Квалифицированного сертификата.....	21

4.3	Подтверждение действительности электронной подписи, использованной для подписания электронных документов .....	21
4.4	Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата.....	22
4.5	Порядок ведения реестра квалифицированных сертификатов .....	24
4.6	Порядок технического обслуживания реестра квалифицированных сертификатов.....	25
5	Порядок исполнения обязанностей Удостоверяющего центра.....	25
5.1	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.....	25
5.2	Выдача по обращению заявителя средств электронной подписи .....	26
5.3	Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий .....	26
5.4	Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов .....	27
5.5	Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей .....	27
5.6	Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации .....	27
5.7	Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации. 28	
5.8	Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов.....	28
6	Сроки действия ключей электронной подписи и сертификата ключа проверки электронной подписи. ....	28
7	Дополнительные положения .....	28
	Приложение № 1 .....	30
	Приложение №2 .....	31
	Приложение №3 .....	32



## **Термины и определения**

В Порядке используются понятия, определенные Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»), а также следующие определения и сокращения:

**Аутентификация** – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности электронной подписи, подтверждение действительности.

**Владелец квалифицированного сертификата ключа проверки электронной подписи (далее Владелец сертификата)** - лицо, которому Удостоверяющим центром выдан квалифицированный сертификат ключа проверки электронной подписи.

**Государственные информационные ресурсы** – совокупность государственных информационных ресурсов, доступ к которым предоставлен Удостоверяющему центру для подтверждения достоверности информации, представленной Заявителем для включения в квалифицированный сертификат.

**Единый портал** – Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)», [www.gosuslugi.ru](http://www.gosuslugi.ru).

**Заявитель** - физическое лицо, обращающееся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

**Ключевой носитель** – носитель, предназначенный для хранения и содержащий ключ электронной подписи и/или дополнительную служебную информацию.

**Компрометация ключа** – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

**Персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

**Сотрудник УЦ** – ответственный сотрудник ООО ИК «СИБИНТЕК», наделенный полномочиями по осуществлению действий по созданию и выдаче сертификатов ключей проверки электронной подписи Заявителям.

**Список прекративших свое действие (аннулированных) сертификатов (далее список отозванных сертификатов (СОС))** – электронный документ с электронной подписью Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, действие которых на определенный момент времени было прекращено или аннулировано.



**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 Общие положения

### 1.1 Предмет регулирования Порядка

Настоящий Порядок реализации функций аккредитованного удостоверяющего центра ООО ИК «СИБИНТЕК» и исполнения его обязанностей (далее - Порядок) определяет порядок и условия предоставления услуг аккредитованного Удостоверяющего центра ООО ИК «СИБИНТЕК» (далее – УЦ или Удостоверяющий центр), включая права, обязанности и ответственность Удостоверяющего центра, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

Настоящий Порядок является договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации.

Присоединение к Порядку осуществляется путем подписания и предоставления Заявителем в Удостоверяющий центр Заявления на создание квалифицированного сертификата ключа проверки электронной подписи по форме, утвержденной в Приложении №1 к настоящему Порядку. Лицо, подавшее Заявление, полностью и безоговорочно соглашается со всеми условиями настоящего Порядка и приложений к нему. Удостоверяющий центр вправе отказать в приеме Заявления на создание квалифицированного сертификата ключа проверки электронной подписи в случае ненадлежащего оформления Заявителем документов, необходимых для оказания услуги, предоставления неактуальных документов или сведений, предоставления их не в полном объеме или предоставления Заявителем не достоверных сведений.

Настоящий Порядок разработан в соответствии с требованиями законодательства Российской Федерации, в том числе следующих нормативно-правовых актов:

- Гражданский кодекс Российской Федерации;
- Федеральный закон Российской Федерации от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных»;
- Федеральный закон от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Приказ ФСБ РФ от 27 декабря 2011 г. №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- Приказ ФСБ РФ от 27 декабря 2011 г. №796 «Об утверждении Требований к средствам электронной подписи и Требованиям к средствам удостоверяющего центра»;
- Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13 ноября 2020 г. №584 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей».

## 1.2 Сведения об Удостоверяющем центре

Полное наименование: Общество с ограниченной ответственностью "СИБИРСКАЯ ИНТЕРНЕТ КОМПАНИЯ"

Сокращенное наименование: ООО ИК "СИБИНТЕК"

Юридический/почтовый адрес: 117152, г. Москва, Шоссе Загородное, д. 1, корпус 1.

ИНН/КПП: 7708119944/997750001

ОГРН: 1027700251314

Банковские реквизиты:

р/с: 40702810900000002089

в БАНК "ВБРР" (АО)

БИК: 044525880

к/с: 30101810900000000880

Адрес электронной почты (e-mail): [ca@sibintek.ru](mailto:ca@sibintek.ru).

Справочный телефон: 8(495) 755-51-17

Адрес осуществления лицензируемого вида деятельности: г. Москва, ш. Загородное, д. 1, к. 1.

График работы: понедельник – пятница, с 9.00 до 17.00 (по московскому времени).

Правовые основания осуществления деятельности на территории Российской Федерации:

- Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России от 14.08.2017 г. серия ЛСЗ №0014921 рег. №16161Н.

## 1.3 Порядок информирования о предоставлении услуг Удостоверяющего центра

Справочный телефон: +7 (495) 517-70-80 (доб.20628)

Адрес электронной почты (e-mail): [ca@sibintek.ru](mailto:ca@sibintek.ru).

Адрес официального сайта в сети Интернет: [www.sibintek.ru](http://www.sibintek.ru).

С актуальной информацией об услугах Удостоверяющего центра можно ознакомиться на официальном сайте в сети Интернет, по справочному телефону или отправив запрос на адрес электронной почты. Срок ответа на запрос по электронной почте – не более 3 (трех) рабочих дней.

Доступ к настоящему Порядку не ограничен. Электронная копия настоящего Порядка размещена на официальном сайте ООО ИК «СИБИНТЕК»: <http://sibintek.ru>.

Внесение изменений (дополнений) в Порядок, в том числе в приложения к нему, производится Удостоверяющим центром в одностороннем порядке. Уведомление Владельцев сертификатов о внесении изменений (дополнений) осуществляется путем размещения (публикации) указанных изменений (дополнений) на официальном сайте Удостоверяющего центра.

Изменения (дополнения), вносимые Удостоверяющим центром в Порядок, кроме изменений (дополнений), вызванных изменением законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон с даты их размещения (публикации) на официальном сайте Удостоверяющего центра.



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

Любые изменения (дополнения) в Порядок с момента вступления их в силу распространяются на всех лиц, присоединившихся к Порядку, в том числе присоединившихся к Порядку ранее даты вступления изменений (дополнений) в силу. Лицо, присоединившееся к Порядку, вправе не согласиться с внесенными изменениями (дополнениями) и расторгнуть Договор с Удостоверяющим центром как это предусмотрено ниже.

Лицо, присоединившееся к Порядку, имеет право в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром в рамках настоящего Порядка, направив в Удостоверяющий центр заявление на прекращение действия сертификата ключа проверки электронной подписи (по форме Приложение №2 к настоящему Порядку) в форме документа на бумажном носителе или в форме электронного документа, с учетом требований п.4.4. настоящего Порядка.

#### **1.4 Стоимость услуг Удостоверяющего центра**

Удостоверяющий центр оказывает услуги на платной основе, за исключением услуг, которые должны предоставляться на безвозмездной основе в соответствии с Федеральным законом «Об электронной подписи». Стоимость услуг Удостоверяющего центра определяется Прейскурантом, размещенным (публикуемым) на официальном сайте Удостоверяющего центра.

Оплата услуг производится в безналичной форме на основании выставленного Удостоверяющим центром счета путем перечисления денежных средств на расчетный счет Удостоверяющего центра в течение 30 (тридцати) календарных дней.

С информацией о стоимости услуг Удостоверяющего центра можно ознакомиться на официальном сайте в сети Интернет, по контактному телефону или отправив запрос на адрес электронной почты. Срок ответа на запрос по электронной почте – не более 3 (трех) рабочих дней.

## **2 Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)**

Удостоверяющий центр реализует следующие функции (услуги):

1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (Заявителям), при условии установления личности получателя сертификата (Заявителя).
2. Осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи.
3. Устанавливает сроки действия сертификатов ключей проверки электронных подписей.

4. Аннулирует выданные удостоверяющим центром сертификаты ключей проверки электронных подписей.
5. Выдает по обращению Заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем.
6. Ведет реестр выданных и аннулированных удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования.
7. Устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет".
8. Создает по обращениям Заявителей ключи электронных подписей и ключи проверки электронных подписей.
9. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов.
10. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.
11. Информировывает 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.
12. Обеспечивает актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
13. Предоставляет 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 ключа проверки электронной подписи.
14. Обеспечивает конфиденциальность созданных удостоверяющим центром ключей электронных подписей.
15. Отказывает Заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата ключа проверки электронной подписи.
16. Отказывает Заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения сертификата ключа проверки электронной подписи.
17. Осуществляет проверку электронных подписей, ключи проверки которых указаны в выданных доверенными лицами сертификатах ключей проверки электронных подписей.



18. Осуществляет иную связанную с использованием электронной подписи деятельность.

### **3 Права и обязанности Удостоверяющего центра**

В рамках оказания услуг Удостоверяющий центр имеет права и обязанности, предусмотренные законодательством Российской Федерации, в том числе, статьями 13 - 15, 17 и 18 Федерального закона "Об электронной подписи":

#### **3.1 Права Удостоверяющего центра**

1. Выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе.
2. Отказать Заявителю в выдаче сертификата ключа проверки электронной подписи в случае невыполнения Заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами.
3. Отказать Заявителю в оказании услуг в случае ненадлежащего оформления Заявления или отсутствия необходимых документов, а также в случае, когда подлинность представленных документов вызывает сомнение.
4. Удостоверяющий центр вправе наделить третьих лиц (далее - доверенные лица) полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра. При совершении порученных удостоверяющим центром действий доверенное лицо обязано идентифицировать Заявителя при его личном присутствии.
5. В одностороннем порядке вносить изменения (дополнения) в Порядок и Прейскурант.

#### **3.2 Обязанности Удостоверяющего центра**

1. Информировать Заявителей об условиях и 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.
2. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
3. 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 ключа проверки электронной подписи.
4. Обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.
5. Отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата ключа проверки электронной подписи.



6. Отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения сертификата ключа проверки электронной подписи.
7. В случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам, уведомить об этом в письменной форме Владельцев сертификатов ключей проверки электронных подписей, которые выданы удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра.
8. В случае прекращения деятельности Удостоверяющего центра с переходом его функций другим лицам, уведомить об этом в письменной форме Владельцев сертификатов ключей проверки электронных подписей, которые выданы удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций.
9. Аннулировать сертификат ключа проверки электронной подписи в следующих случаях:
  - Не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате.
  - Установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи.
  - Вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.
10. Внести информацию о прекращении действия сертификата ключа проверки электронной подписи в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.
11. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи, уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.
12. Хранить в течение срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативно-правовыми актами Российской Федерации, следующую информацию:
  - реквизиты основного документа, удостоверяющего личность Владельца квалифицированного сертификата - физического лица;
  - информацию, подтверждающую ознакомление Заявителя с информацией, содержащейся в квалифицированном сертификате.
13. Для подписания от своего имени квалифицированных сертификатов использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

14. Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов Удостоверяющего центра в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.
15. В случае принятия решения о прекращении своей деятельности:
  - сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;
  - передать в уполномоченный федеральный орган в установленном порядке реестр выданных Удостоверяющим центром квалифицированных сертификатов;
  - передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в Удостоверяющем центре.
16. При выдаче квалифицированного сертификата идентифицировать Заявителя - физическое лицо, обратившееся в удостоверяющий центр за получением квалифицированного сертификата. Идентификация Заявителя проводится при его личном присутствии или посредством идентификации Заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации Заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном законодательством РФ. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, Удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

В отношении физического лица устанавливаются - фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования.
17. Предложить использовать шифровальные (криптографические) средства физическим лицам, обратившимся в Удостоверяющий центр в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти



средства. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

18. Подтвердить достоверность сведений, перечисленных в пунктах 1 и 2 части 1 статьи 18 Федерального закона «Об электронной подписи» одним из следующих способов:
  - 1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;
  - 2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;
  - 3) с использованием единой системы идентификации и аутентификации.
19. С использованием государственных информационных ресурсов осуществить проверку достоверности документов и сведений, представленных Заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона «Об электронной подписи».
20. При выдаче квалифицированного сертификата направить 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).
21. При выдаче квалифицированного сертификата по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию указанного лица в единой системе идентификации и аутентификации.
22. Исполнять иные обязанности, предусмотренные настоящим Порядком, Федеральным законом "Об электронной подписи", другими нормативными правовыми актами.

### **3.3 Права Владельца сертификата**

1. Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Удостоверяющим центром.
2. Обратиться в Удостоверяющий центр для прекращения действия квалифицированного сертификата в течение срока действия соответствующего ключа электронной подписи.
3. Обратиться в Удостоверяющий центр за подтверждением подлинности электронной подписи в электронных документах и получения других услуг.
4. Осуществлять иные права, предусмотренные для Владельца сертификата настоящим Порядком и действующим законодательством РФ.



### **3.4 Обязанности Владельцев квалифицированного сертификата**

Владелец сертификата обязан:

1. Не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр для прекращения действия сертификата ключа электронной подписи при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.
2. Исполнять иные обязанности, предусмотренные для Владельца сертификата настоящим Порядком и действующим законодательством РФ.

### **3.5 Права Заявителя**

Заявитель имеет право:

1. По собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 2 - 6 части 2 статьи 18 Федерального закона «Об электронной подписи».
2. Получать достоверные сведения об Удостоверяющем центре, перечне, стоимости и порядке оказания услуг Удостоверяющего центра.
3. Осуществлять иные права, предусмотренные для Заявителей настоящим Порядком и действующим законодательством РФ.

### **3.6 Обязанности Заявителя**

1. При обращении в Удостоверяющий центр Заявитель обязан представить следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:
  - а) основной документ, удостоверяющий личность;
  - б) страховой номер индивидуального лицевого счета Заявителя;
  - с) идентификационный номер налогоплательщика Заявителя.
2. Исполнять иные обязанности, предусмотренные для Заявителей настоящим Порядком и действующим законодательством РФ.

## **4 Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром**

### **4.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей**

#### **4.1.1 Порядок создания ключей электронных подписей и ключей проверки электронных подписей**

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется:

1. Заявителями самостоятельно. При этом Заявитель должен создавать ключи электронной подписи и ключи 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)»;

2. Сотрудниками Удостоверяющего центра по Заявлению, представленному в Удостоверяющий центр, 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), с сохранением в тайне изготовленного ключа электронной подписи.

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 «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также при условии выполнения требований, установленных Постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи.

#### **4.1.2 Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра. Порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены**

##### **4.1.2.1 Плановая смена**

Плановая смена ключей электронной подписи 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 ключа электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

1. Удостоверяющий центр формирует новый ключ электронной подписи, соответствующий ему ключ проверки электронной подписи и запрос на сертификат удостоверяющего центра.
2. Сформированный запрос на сертификат направляется в уполномоченный федеральный орган в области использования электронной подписи.
3. Уполномоченный федеральный орган в области использования электронной подписи выдает удостоверяющему центру квалифицированный сертификат, созданный с использованием средств головного удостоверяющего центра.

Ключ электронной подписи Удостоверяющего центра, подлежащий замене, используется до окончания срока действия последнего выпущенного сертификата Удостоверяющего центра на этом ключе электронной подписи Удостоверяющего центра для формирования списков отозванных сертификатов в электронной форме.



#### 4.1.2.2 Внеплановая смена

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего центра, а также в иных случаях по инициативе Удостоверяющего центра.

Под компрометацией (нарушением конфиденциальности) ключа электронной подписи Удостоверяющего центра понимается хищение, утрата, разглашение, несанкционированное копирование и другие события, в результате которых ключ электронной подписи может стать доступным несанкционированным лицам и (или) процессам. К событиям, связанным с компрометацией ключа электронной подписи, относятся, включая, но не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с их последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- 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).

Под случаями угрозы компрометации (нарушения конфиденциальности) ключа электронной подписи Удостоверяющего центра понимается возможность реализации воздействия на ключи электронной подписи, приводящего к искажению, уничтожению, копированию, блокированию и/или доступа к ключам электронной подписи.

Процедура внеплановой смены ключей электронной подписи Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра.

В случае проведения внеплановой смены ключей из-за компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего центра, после выполнения процедуры внеплановой смены ключей электронной подписи Удостоверяющего центра, сертификат ключа проверки электронной подписи Удостоверяющего центра аннулируется путем занесения в список отозванных сертификатов, в связи с этим прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

**4.1.3 Информирование о смене ключей электронной подписи Удостоверяющего центра**  
Удостоверяющий центр информирует Владельцев сертификатов о факте смены ключей Удостоверяющего центра посредством размещения информации на официальном сайте Удостоверяющего центра.

Доверенными способами получения нового квалифицированного сертификата Удостоверяющего центра является:



- получение Заявителем квалифицированного сертификата в Удостоверяющем центре непосредственно в Удостоверяющем центре;
- загрузка квалифицированного сертификата Удостоверяющего центра с официального сайта Удостоверяющего центра.

#### **4.1.4 Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Владельца квалифицированного сертификата.**

Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона «Об электронной подписи».

Порядок смены ключей электронной подписи Владельца сертификата, а также, требования к заявлению на смену ключа электронной подписи Владельца сертификата, в том числе, состав реквизитов такого заявления, определяются действующим законодательством и настоящим Порядком, в соответствии с процедурой создания ключей электронной подписи и ключей проверки электронных подписей.

Заявление на смену ключа электронной подписи Владельца сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Владельца этого 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 квалифицированного сертификата и ключа электронной подписи (при необходимости) владельцу, в том числе в электронной форме, осуществляется в соответствии положениями статьи 18 Федерального закона «Об электронной подписи».

## **4.2 Процедура создания и выдачи квалифицированных сертификатов**

### **4.2.1 Порядок подачи заявления на создание и выдачу квалифицированных сертификатов**

Удостоверяющий центр обеспечивает создание квалифицированного сертификата ключа проверки электронной подписи по заявлению на создание квалифицированного сертификата ключа проверки электронной подписи, в соответствии с порядком идентификации Владельца сертификата ключа проверки электронной подписи, определённым в настоящем Порядке. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи определяется Приложением №1 к настоящему Порядку (далее – Заявление).

### **4.2.2 Требования к заявлению на создание и выдачу квалифицированных сертификатов**

Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми

Правительством Российской Федерации<sup>1</sup>, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее - единая система идентификации и аутентификации)<sup>2</sup> и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных" (далее - единая биометрическая система)<sup>3</sup>.

Подписание Заявления на бумажном носителе производится собственноручно лицом, сведения о котором содержатся в Заявлении. Использование факсимиле (клише подписи) на Заявлении не допускается.

В случае если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Сертификат выдается при личном прибытии в Удостоверяющий центр Владельца сертификата, либо без его личного присутствия одним из способов, указанных в абзаце первом пункта 1 части 1 статьи 18 Федерального закона «Об электронной подписи».

#### 4.2.3 Порядок идентификации Заявителя (установления личности)

Идентификация Заявителя проводится при его личном присутствии или посредством идентификации Заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации Заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном законодательством РФ. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от

<sup>1</sup> Постановление Правительства Российской Федерации от 25 января 2013 г. № 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг".

<sup>2</sup> Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

<sup>3</sup> Пункт 4 статьи 2 Федерального закона от 29 декабря 2022 г. № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации".



использования шифровальных (криптографических) средств, Удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

Идентификацию Заявителя при его личном присутствии Удостоверяющий центр осуществляет следующим образом:

- 1) Идентификация гражданина Российской Федерации осуществляется по основному документу, удостоверяющему личность;
- 2) Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;
- 3) Идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

#### **4.2.4 Перечень документов, запрашиваемых Удостоверяющим центром у Заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности Заявителя**

Для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности Заявителя, Заявитель предоставляет документы, перечень которых установлен в части 2 статьи 18 Федерального закона «Об электронной подписи».

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

Если для подтверждения сведений, вносимых в Квалифицированный сертификат, действующим законодательством установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом.

#### **4.2.5 Порядок проверки достоверности документов и сведений**

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона «Об электронной подписи» Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона «Об электронной подписи».

В случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат и Удостоверяющим центром идентифицирован Заявитель, Удостоверяющий центр осуществляет процедуру создания и выдачи Заявителю квалифицированного сертификата. В противном случае, а также в случаях, установленных пунктами 5 и 6 части 2 статьи 13 Федерального закона «Об электронной подписи», удостоверяющий центр отказывает Заявителю в выдаче квалифицированного сертификата.

#### **4.2.6 Порядок создания квалифицированного сертификата**

Создание квалифицированного сертификата осуществляется Удостоверяющим центром в соответствии с положениями статей 13-15, 17 и 18 Федерального закона «Об электронной подписи» и настоящим Порядком.

В квалифицированный сертификат вносится информация на основании данных, указанных в Заявлении.

Удостоверяющий центр проверяет данные в Заявлении и устанавливает:

- факт принадлежности документов предоставившему их лицу;
- факт соответствия сведений, указанных в Заявлении, представленным документам и информации, полученной из государственных информационных ресурсов;
- факт отсутствия явных признаков подделки документов.

В случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в квалифицированный сертификат, и Удостоверяющим центром установлена личность Заявителя, Удостоверяющий центр создает квалифицированный сертификат ключа проверки электронной подписи и ключ электронной подписи (при необходимости).

Формат и структура создаваемого квалифицированного сертификата ключа проверки электронной подписи соответствуют требованиям Федерального закона «Об электронной подписи» и Приказа ФСБ России от 27 декабря 2011 г. №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Удостоверяющий центр на основаниях, предусмотренных действующим законодательством РФ и настоящим Порядком, вправе отказать Заявителю в создании квалифицированного сертификата. Информация о причинах отказа предоставляется Заявителю путем направления электронного письма на адрес электронной почты, указанный Заявителем в Заявлении.

#### **4.2.7 Порядок выдачи квалифицированного сертификата**

При получении квалифицированного сертификата Заявителем он должен быть ознакомлен Удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования Заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи Заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью



данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление Заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности, если более короткий срок не предусмотрен нормативно-правовыми актами Российской Федерации.

После ознакомления Заявителя с информацией, внесенной в Сертификат и получения соответствующей расписки Удостоверяющий центр выдает Заявителю:

- ключ электронной подписи и квалифицированный сертификат (с ключом проверки ЭП);
- сертификат Головного удостоверяющего центра и сертификат Удостоверяющего центра, использовавшийся для подписи квалифицированного сертификата;
- копию квалифицированного сертификата на бумажном носителе (по запросу).

Одновременно с выдачей квалифицированного сертификата Удостоверяющий центр предоставляет Владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Факт создания ключа электронной подписи и соответствующего ему ключа проверки электронной подписи, содержащегося в квалифицированном сертификате, Удостоверяющим центром, или факт создания данных ключей Заявителем самостоятельно при помощи Средств электронной подписи, выданных ему Удостоверяющим центром, подтверждает факт владения Владельцем квалифицированного сертификата ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате.

Факт ознакомления Владельца квалифицированного сертификата с информацией, содержащейся в сертификате, является фактом получения квалифицированного сертификата его Владельцем.

#### **4.2.8 Срок создания и выдачи Квалифицированного сертификата**

Срок создания и выдачи Квалифицированного сертификата не должен превышать 5 (пяти) рабочих дней с момента получения Удостоверяющим центром соответствующего Заявления и корректного комплекта документов, при условии получения подтверждения информации, содержащейся в Заявлении, в государственных информационных ресурсах.

Срочное создание и выдача Квалифицированного сертификата не производится.

#### **4.3 Подтверждение действительности электронной подписи, использованной для подписания электронных документов**

Подтверждение действительности электронной подписи в электронном документе осуществляется на основании заявления на подтверждение действительности электронной подписи в электронном документе, форма которого установлена Приложение №3 к настоящему Порядку (далее - Заявление на подтверждение действительности ЭП).

Обязательным приложением к Заявлению на подтверждение действительности ЭП является съемный носитель информации (usb drive, cd-rom), содержащий следующие файлы:

- файл, содержащий электронный документ, к которому применена электронная подпись;
- файл, содержащий электронную подпись формата PKCS#7 электронного документа, к которому применена электронная подпись;

Удостоверяющий центр оказывает услугу по подтверждению действительности электронной подписи в электронном документе в срок не более 15 (пятнадцати) рабочих дней с момента предоставления в Удостоверяющий центр Заявления на подтверждение действительности ЭП. Заявление на подтверждение действительности ЭП подается в офис Удостоверяющего центра Заявителем лично.

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

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, всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром.;
- проверка отсутствия сертификатов в списках отозванных сертификатов (CRL).

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

Заключение предоставляется в форме электронного документа, заверенного усиленной квалифицированной электронной подписью сотрудника Удостоверяющего центра.

#### **4.4 Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата**

Квалифицированный сертификат ключа проверки электронной подписи прекращает свое действие в случаях, установленных статьей 14 Федерального закона «Об электронной подписи». В случае прекращения срока действия квалифицированного сертификата никаких дополнительных действий не требуется.



Удостоверяющий центр признает квалифицированный сертификат аннулированным, если:

1. Не подтверждено, что Владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;
2. Установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;
3. Вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию.

В случае необходимости прекращения действия квалифицированного сертификата ключа проверки электронной подписи по обращению Владельца квалифицированного сертификата ключа проверки электронной подписи, Владелец сертификата должен сформировать заявление на прекращение действия квалифицированного сертификата ключа проверки электронной подписи (по форме Приложения №2 к настоящему Порядку) на бумажном носителе или в форме электронного документа, при этом заявление должно обязательно содержать:

- сведения о Владельце сертификата, действие которого прекращается (фамилия имя и отчество, страховой номер индивидуального лицевого счета (СНИЛС), идентификационный номер налогоплательщика (ИНН));
- сведения о квалифицированном сертификате, действие которого прекращается;
- причину прекращения действия квалифицированного сертификата;
- наименование аккредитованного удостоверяющего центра;
- дату подписания заявления;
- собственноручную подпись Владельца сертификата или усиленную квалифицированную электронную подпись Владельца сертификата.

С заявлением о прекращении действия квалифицированного сертификата физического лица, может лично обращаться физическое лицо, которое является Владельцем этого квалифицированного сертификата.

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.

При проведении идентификации (установления) личности Владельца сертификата Удостоверяющий центр руководствуется п. 4.2.3. настоящего Порядка.

Заявление о прекращении действия квалифицированного сертификата может быть направлено в Удостоверяющий центр как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, в том числе с использованием Единого портала ([www.gosuslugi.ru](http://www.gosuslugi.ru)).

После проверки заявления и полномочий Владельца сертификата, обратившегося для прекращения действия квалифицированного сертификата, Удостоверяющий центр:

- выполняет процедуру прекращения действия квалифицированного сертификата;
- вносит информацию о прекращении действия квалифицированного сертификата в список отозванных сертификатов удостоверяющего центра;
- вносит информацию о прекращении действия квалифицированного сертификата в реестр сертификатов удостоверяющего центра.

Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата ключа проверки электронной подписи в реестр квалифицированных сертификатов не может превышать 12 (двенадцать) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

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

В случае, если заявление о прекращении действия квалифицированного сертификата не соответствует требованиям настоящего раздела, в том числе в случае, если квалифицированный сертификат, сведения о котором указаны в заявлении, не выдавался Удостоверяющим центром, либо сведения, указанные в заявлении, не соответствуют сведениям о Владельце сертификата, либо не подтверждены полномочия лица, обратившегося с заявлением, Удостоверяющий центр отказывает в проведении процедуры прекращения действия квалифицированного сертификата и направляет соответствующее уведомление лицу, направившему заявление, в течение 3 (трех) рабочих дней со дня получения заявления о прекращении действия квалифицированного сертификата с использованием электронной почты на электронный адрес Владельца сертификата, известный Удостоверяющему центру. Если квалифицированный сертификат, сведения о котором указаны в заявлении, не выдавался Удостоверяющим центром, Удостоверяющий центр вправе не уведомлять лицо, обратившегося с заявлением.

#### **4.5 Порядок ведения реестра квалифицированных сертификатов**

Реестр квалифицированных сертификатов ведется в соответствии с Приказом Минцифры России от 08.11.2021 №1138 "Об утверждении Порядка формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов



ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации".

Сведения о прекращении действия или аннулирования квалифицированных сертификатов вносятся Удостоверяющим центром в реестр квалифицированных сертификатов в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в 6 и 6.1. статьи 14 Федерального закона «Об электронной подписи», или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи в реестр квалифицированных сертификатов.

Реестр выданных квалифицированных сертификатов ведется в электронной форме в формате базы данных с использованием средств Удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Формат списка аннулированных (отозванных) сертификатов соответствует стандарту X.509 версии 2. Информация о адресах публикации списка аннулированных (отозванных) сертификатов указывается в квалифицированных сертификатах, созданных Удостоверяющим центром, и включается в расширение «Точка распределения списка отзыва» («CRL Distribution Point») квалифицированного сертификата.

Квалифицированный сертификат считается аннулированным с момента внесения записи в реестр квалифицированных сертификатов.

#### **4.6 Порядок технического обслуживания реестра квалифицированных сертификатов**

Максимальный срок планового технического обслуживания составляет 3 (три) часа. Внеплановое техническое обслуживание проводится по необходимости. Срок проведения внепланового технического обслуживания составляет не более 8 (восьми) часов. Срок проведения внепланового технического обслуживания может быть увеличен по объективным причинам, но не более, чем до 48 (сорока восьми) часов.

Уведомление участников информационного взаимодействия о проведении технического обслуживания осуществляется посредством публикации соответствующей информации на официальном сайте Удостоверяющего центра.

### **5 Порядок исполнения обязанностей Удостоверяющего центра**

#### **5.1 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**

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 осуществляется путем предоставления «Руководства по обеспечению безопасности

использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» одновременно с выдачей квалифицированного сертификата.

## **5.2 Выдача по обращению заявителя средств электронной подписи**

Средства электронной подписи, должны соответствовать требованиям части 4 статьи 6 Федерального закона «Об электронной подписи» и 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.

## **5.3 Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий**

Актуальность информации, содержащейся в реестре квалифицированных сертификатов, обеспечивается регулярным обновлением данных Удостоверяющим центром, в том числе, путем соблюдения сроков внесения сведений о прекращении действия и/или аннулировании Сертификатов, установленных Федеральным законом «Об электронной подписи».

Обеспечение защиты информации, содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается в соответствии с требованиями действующего законодательства и достигаются путем принятия следующих мер:

- 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, исключаяющей свободное пребывание посторонних лиц;
- использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.



#### **5.4 Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов**

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к Реестру квалифицированных сертификатов на официальном сайте Удостоверяющего центра.

Реестр квалифицированных сертификатов доступен круглосуточно и ежедневно, за исключением времени проведения технического обслуживания.

Прием запросов на предоставление информации о действующих квалифицированных сертификатах, выданных Удостоверяющим центром, по электронной почте осуществляется круглосуточно.

#### **5.5 Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей**

Конфиденциальность созданных Удостоверяющим центром ключей электронных подписей обеспечивается в соответствии с требованиями эксплуатационной документации на средства электронной подписи и законодательства РФ. Для создания ключа электронной подписи Удостоверяющим центром используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

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 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 сертификата.

Удостоверяющий центр не осуществляет временное хранение ключей электронных подписей Владельцев сертификатов (Заявителей).

#### **5.6 Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации**

Регистрация квалифицированного сертификата в единой системе идентификации и аутентификации осуществляется при выдаче квалифицированного сертификата, путем направления в единую систему идентификации и аутентификации сведений о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате.

### **5.7 Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации**

При выдаче квалифицированного сертификата Удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

### **5.8 Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов**

Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению доступ к реестру сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, путем публикации реестра сертификатов на официальном сайте Удостоверяющего центра.

Адрес публикации списка отозванных сертификатов Удостоверяющего центра указывается в квалифицированных сертификатах, созданных Удостоверяющим центром.

## **6 Сроки действия ключей электронной подписи и сертификата ключа проверки электронной подписи.**

Срок действия ключа проверки электронной подписи устанавливается равным сроку действия сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи составляет 12 месяцев.

## **7 Дополнительные положения**

Удостоверяющий центр и Заявители, обратившиеся в Удостоверяющий центр, в процессе обмена электронными документами обязуются обеспечить сохранность конфиденциальной информации, полученной друг от друга в соответствии с действующим законодательством Российской Федерации.

Заявитель поручает Удостоверяющему центру обрабатывать свои персональные данные в целях исполнения договора, в частности хранить, публиковать сведения, включающиеся в сертификат проверки ключей электронной подписи, использовать персональные данные для идентификации.

Порядок предоставления конфиденциальной информации налоговым, правоохранительным и судебным органам осуществляется в соответствии с действующим законодательством Российской Федерации.

За неисполнение или ненадлежащее исполнение обязанностей по настоящему Порядку Владельцы сертификатов несут ответственность в соответствии с действующим законодательством Российской Федерации и настоящим Порядком.



Заявитель несет ответственность за достоверность сведений, указанных им в заявлении и достоверность иных документов, предоставляемых в Удостоверяющий центр в соответствии с настоящим Порядком и действующим законодательством.

Заявитель несет ответственность за сохранность и правильность эксплуатации средств электронной подписи, а также за сохранность своих ключей электронной подписи.

Удостоверяющий центр не несёт ответственности перед владельцами сертификатов ключей проверки электронной подписи за любые убытки, потери, иной ущерб, связанный с использованием сертификатов ключей проверки электронной подписи, независимо от суммы заключенных с использованием ключей проверки электронной подписи сделок и совершения ими иных действий, за исключением случаев неисполнения или ненадлежащего исполнения Удостоверяющим центром обязательств, предусмотренных настоящим Порядком и/или действующим законодательством Российской Федерации.

Удостоверяющий центр не несет ответственности за невозможность использования сертификата в случае, если такая невозможность возникла после создания сертификата и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

При исполнении своих обязательств по настоящему Порядку, Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или на иные неправомерные цели.

Стороны подтверждают, что ознакомились с содержанием и обязуются придерживаться принципов Политики Компании «В области противодействия корпоративному мошенничеству и вовлечению в коррупционную деятельность», размещенной в открытом доступе на официальном сайте ПАО «НК «Роснефть» в сети Интернет.

## Приложение № 1

### Заявление на создание квалифицированного сертификата ключа проверки электронной подписи

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

Согласно Порядку реализации функций удостоверяющего центра ООО ИК «СИБИНТЕК» прошу создать квалифицированный сертификат ключа проверки электронной подписи согласно следующим регистрационным данным:

<b>Общее имя (CommonName)</b>	<b>ФИО (Обязательное поле)</b>
<b>Фамилия (surname)</b>	<b>Фамилия (Обязательное поле)</b>
<b>Имя и отчество (givenName)</b>	<b>Имя и отчество (Обязательное поле)</b>
<b>Улица, дом (streetAddress)</b>	<b>Адрес (По желанию заявителя)</b>
<b>Город (localityName)</b>	<b>Город (По желанию заявителя)</b>
<b>Область, край (stateOrProvinceName)</b>	<b>Область (По желанию заявителя)</b>
<b>Страна (countryName)</b>	<b>RU</b>
<b>Электронная почта (E-Mail (E))</b>	<b>Почта (По желанию заявителя)</b>
<b>ИНН (INN)</b>	<b>ИНН (Обязательное поле)</b>
<b>Страховой номер индивидуального лицевого счета (СНИЛС) (SNILS)</b>	<b>СНИЛС (Обязательное поле)</b>

Сведения о владельце сертификата ключа проверки электронной подписи, необходимые для направления в единую систему идентификации и аутентификации:

<b>Пол</b>	
<b>Гражданство</b>	
<b>Дата рождения</b>	
<b>Место рождения</b>	
<b>Вид основного документа, удостоверяющего личность</b>	
<b>Серия</b>	
<b>Номер</b>	
<b>Дата выдачи</b>	
<b>Дата окончания действия</b>	
<b>Код подразделения</b>	

Настоящим я, \_\_ **ФИО** **Серия и номер паспорта** \_\_\_\_\_,  
(**ФИО, паспортные данные владельца сертификата**)

выражаю согласие на обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение) своих персональных данных (с использованием средств автоматизации и без использования таких средств) удостоверяющим центром ООО ИК «СИБИНТЕК» и его доверенными лицами. Согласие предоставляется с целью оказания услуг удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 №63-ФЗ.

Срок действия настоящего согласия – период времени до истечения установленных нормативными актами сроков хранения соответствующей информации или документов, а в случаях, когда такие сроки не установлены – до достижения целей обработки соответствующих персональных данных. Отзыв согласия совершается путем подачи его в письменной форме.

Настоящим присоединяюсь к условиям Порядка реализации функций удостоверяющего центра ООО ИК «СИБИНТЕК», расположенного на сайте УЦ по адресу <http://sibintek.ru/> и принимаю на себя обязательства следовать его положениям, которое понятны и приняты мною в полном объеме и имеют для меня обязательную силу.

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
**ФИО**

Отметка сотрудника УЦ о принятии заявления

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
«\_\_\_» \_\_\_\_\_ 20\_\_ г.



## Приложение №2

**В удостоверяющий центр  
ООО ИК «СИБИНТЕК»**

### Заявление на прекращение действия сертификата ключа проверки ЭП

от \_\_\_\_\_

ФИО

\_\_\_\_\_ 20\_\_

Прошу прекратить действие квалифицированного сертификата ключа проверки электронной подписи, серийный номер: \_\_\_\_\_, выданный на имя:

<b>Фамилия Имя Отчество</b>	<b>ФИО (Обязательное поле)</b>
<b>ИНН (INN)</b>	<b>ИНН (Обязательное поле)</b>
<b>Страховой номер индивидуального лицевого счета (СНИЛС) (SNILS)</b>	<b>СНИЛС (Обязательное поле)</b>

в связи с \_\_\_\_\_ (причина  
прекращения действия сертификата ключа проверки электронной подписи.

\_\_\_\_\_ / \_\_\_\_\_ /

ФИО

## Приложение №3

### Заявление на подтверждение подлинности ЭП в электронном документе

Прошу подтвердить действительность электронной подписи в документе

\_\_\_\_\_ (указать наименование документа и указать имя файла)

Серийный номер сертификата: \_\_\_\_\_,  
сертификат выдан на имя: \_\_\_\_\_

(ФИО Владельца сертификата)

В ходе проверки также прошу установить статус этого сертификата (действовал/не действовал) на момент подписания документа.

3. Время, на момент наступления которого требуется подтвердить подлинность ЭП (учетом часового пояса г. Москвы):

« \_\_\_\_\_ : \_\_\_\_\_ » « \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_ »;  
час            минута            день            месяц            год

\_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

ФИО