



УТВЕРЖДАЮ

И.о. Председателя Правления

ПАО «Совкомбанк»

И.Н. Кашина / И.Н. Кашина/

«19» февраля 2025 года



Приложение №1

к Приказу №206_ОД от 19.02.2025

РЕГЛАМЕНТ (ПОРЯДОК)
ОКАЗАНИЯ УСЛУГ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ПАО «СОВКОМБАНК»

г. Кострома
2025

СОДЕРЖАНИЕ

1	ОБЩИЕ ПОЛОЖЕНИЯ	2
1.1.	Предмет регулирования	2
1.2.	Присоединение к Порядку. Заключение договора на оказание услуг Удостоверяющего центра.....	2
1.3.	Изменения (дополнения) Порядка	2
1.4.	Сведения об Удостоверяющем центре	2
1.5.	Порядок информирования о предоставлении услуг Удостоверяющего центра.....	3
1.6.	Стоимость услуг Удостоверяющего центра, сроки и порядок расчетов.....	3
2	ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ	5
3	ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ	7
4	ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА. ОТВЕТСТВЕННОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	8
4.1.	Права Удостоверяющего центра	8
4.2.	Обязанности Удостоверяющего центра	8
4.3.	Ответственность Удостоверяющего центра.....	10
5	ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СЕРТИФИКАТА.....	11
5.1.	Обязанности Заявителя	11
5.2.	Права Владельца сертификата	11
5.3.	Обязанности Владельца сертификата.....	11
6	ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ	12
6.1.	Права Участников электронного взаимодействия	12
6.2.	Обязанности Участников электронного взаимодействия.....	12
7	ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ	13
7.1.	Процедура создания ключей электронных подписей и ключей проверки электронных подписей	13
7.2.	Процедура создания и выдачи Сертификатов	15
7.3.	Подтверждение действительности электронной подписи, использованной для подписания электронных документов.....	18
7.4.	Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата	18
7.5.	Порядок ведения реестра Сертификатов.....	19
7.6.	Порядок технического обслуживания Реестра сертификатов.....	20
8	ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	21
9	СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ И СЕРТИФИКАТОВ	23

ПРИЛОЖЕНИЯ:

Приложение №1 – 14.02.127_02_Заявление на создание и выдачу сертификата ключа проверки электронной подписи;

Приложение №2 – 14.02.127_05_Форма заявления на прекращение действия квалифицированного сертификата ключа проверки электронной подписи для физических лиц

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 настоящим Порядком на сайте по адресу <https://sovcombank.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 создание и выдачу ключа проверки электронной подписи по форме, утвержденной в Приложение №1 к Порядку (далее – Заявление на выдачу Сертификата), присоединяется к настоящему Порядку 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 квалифицированного сертификата ключа проверки электронной подписи для физических лиц выданного ему Сертификата по форме, утвержденной в Приложении №2 к Порядку (далее – Заявление на прекращение 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://sovcombank.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://sovcombank.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.

1.4. 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. Публичное акционерное общество «Совкомбанк» (ИНН/КПП 4401116480/440101001), именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Костроме.

1.4.3. Удостоверяющий центр в качестве участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской Федерации на основании следующих документов:

- лицензии Управления Федеральной службы безопасности Российской Федерации по Костромской области от 22.11.2019 рег. №Л051-00105-44/00559823 на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области

шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица и индивидуального предпринимателя).

1.4.4. Юридический адрес и фактическое местонахождение Удостоверяющего центра: 620017, г. Кострома, проспект Текстильщиков, д. 46.

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://sovcombank.ru/>.

1.5. Порядок информирования о предоставлении услуг Удостоверяющего центра

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

1) по контактному номеру телефона: тел.: 8 (495) 411-54-14, 8 (800) 200-54-14

2) по адресу электронной почты: e-mail: skbca@sovcombank.ru;

3) путем опубликования информации на официальном сайте: <https://sovcombank.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://sovcombank.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://sovcombank.ru/>.

1.6. Стоимость услуг Удостоверяющего центра, сроки и порядок расчетов

1.6.1. Удостоверяющий центр осуществляет свою деятельность на платной основе.

1.6.2. Стоимость и состав услуг Удостоверяющего центра устанавливается 08.00.157_Тарифами на услуги Удостоверяющего центра ПАО «Совкомбанк» для клиентов (далее – Тарифы на услуги УЦ).

1.6.3. Информирование о стоимости услуг Удостоверяющего центра осуществляется путем опубликования Тарифов на услуги УЦ в информационно-телекоммуникационной сети «Интернет» по адресу: <https://sovcombank.ru/>.

1.6.4. Сторона, присоединившаяся к Порядку, уплачивает Удостоверяющему центру вознаграждение на основании счета, выставленного Удостоверяющим центром.

1.6.5. Оплата осуществляется авансовым платежом в размере 100% (Ста процентов) стоимости в российских рублях в безналичной форме по реквизитам Удостоверяющего центра, указанным в выставленном Удостоверяющим центром счете. Датой оплаты считается дата поступления денежных средств на счет Удостоверяющего центра.

1.6.6. Для своевременной идентификации платежа Заявителя платежное поручение в графе «Назначение платежа» должно содержать ИНН Заявителя, реквизиты счета с указанием назначения платежа.

1.6.7. Заявителю доступны следующие способы получения документов по оказанным услугам: посредством системы электронного документооборота (при условии, что от Заявителя получено согласие на обмен документами по оказанным услугам в электронном виде с указанием системы электронного документооборота), либо на бумажном носителе путем направления документов Удостоверяющим центром почтовой связью.

1.6.8. В случае нарушения Заявителем любого из положений настоящего Порядка и приложений к нему в отношении оплаты вознаграждения Удостоверяющего центра в полном объеме, последний имеет право не оказывать Заявителю услуги до исполнения Заявителем обязательств по Порядку надлежащим образом. В этом случае риск возможных убытков Заявителя полностью ложится на Заявителя (п. 1. ст. 406 части первой Гражданского Кодекса Российской

Федерации).

1.6.9. Услуги Удостоверяющего центра считаются оказанными, если Заявитель не предъявил претензий в письменном виде по их качеству и объему в течение 3 (Трех) рабочих дней со дня их оказания, с обязательным предварительным уведомлением Удостоверяющего центра о выставлении претензии по факсимильной связи, электронной почте или с использованием других средств связи.

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

1.6.11. 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.

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

2. ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

2.1. 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.

2.2. 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 настоящему Порядку.

2.3. Единая биометрическая система - государственная информационная система "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных", которая содержит биометрические персональные данные физических лиц и иную информацию, которая используется в целях осуществления идентификации, аутентификации с использованием биометрических персональных данных физических лиц.

2.4. Единая система идентификации и аутентификации (ЕСИА) — Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

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

2.6. Информационная система (ИС) – программно-аппаратный комплекс и информационный сервис, имеющие адрес в информационно-телекоммуникационной сети «Интернет»: <https://fintender.ru/>, с помощью которых Оператор ИС, Удостоверяющий центр и Заявители осуществляют обмен документами и сведениями, связанными с изготовлением, получением, приостановлением и аннулированием Квалифицированного сертификата ключа проверки электронной подписи.

2.7. 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.

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

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

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

2.11. Оператор ИС – Акционерное общество «Финтендер» (ИНН 7743113487, ОГРН 1157746705930).

2.12. 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.

2.13. 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. По тексту настоящего Порядка употребление термина «Сертификат» означает Сертификат КЭП

2.14. 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».

2.15. 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».

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

2.17. Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме физические лица.

2.18. 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.

2.19. Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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.

3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

3.1. Создание и выдача Сертификатов в электронной форме.

3.2. Изготовление заверенных копий Сертификатов на бумажном носителе по запросу.

3.3. Осуществление подтверждения владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному для получения Сертификата.

3.4. Установление сроков действия Сертификатов.

3.5. 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.

3.6. Выдача Средств электронной подписи, обеспечивающих возможность создания Ключа электронной подписи и Ключа проверки.

3.7. Ведение Реестра сертификатов.

3.8. Установление порядка ведения Реестра сертификатов КЭП.

3.9. Создание Ключей проверки и Ключей электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи.

3.10. Проверка уникальности Ключей проверки в Реестре сертификатов.

3.11. Проверка действительности ЭП, Ключи проверки которых содержатся в Сертификатах, выданных Удостоверяющим центром, в Электронных документах.

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

3.13. Выдача инструкций по информационной безопасности, содержащих условия и порядок использования сертификатов ЭП, ключей ЭП и средств ЭП.

3.14. Информирование лиц, обращающихся в Удостоверяющий центр для выдачи Сертификата, о рисках, связанных с использованием ЭП.

3.15. Предоставление возможности Заявителю создать Ключи проверки и Ключи электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи в Центрах выдачи, имеющих необходимые лицензии.

3.16. Представление по запросу Участников электронного взаимодействия Сертификатов, внесённых в Реестр сертификатов Удостоверяющего центра, в форме электронных документов.

3.17. Выполнение иных функций, установленных действующим законодательством Российской Федерации.

4. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА. ОТВЕТСТВЕННОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1. Права Удостоверяющего центра

4.1.1. 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.

4.1.2. 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.

4.1.3. Обработать персональные данные Заявителя с использованием технических средств.

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

4.1.5. 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.

4.1.6. Отказать в выдаче Сертификата в случае подачи Заявления на выдачу Сертификата с ошибками, исправлениями, подчистками и/или приписками, не подтвержденными собственноручной подписью Заявителя.

4.1.7. Отказать в выдаче Сертификата в случае, если Заявитель не предоставил письменного согласия на обработку своих персональных данных.

4.1.8. 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.

4.1.9. Отказать в выдаче Сертификата в случае, если Заявитель не согласился с обработкой и хранением персональных данных с помощью технических средств.

4.1.10. Отказать в выдаче Сертификата в случае, если Заявитель в течение 30 календарных дней с момента поступления на счет Удостоверяющего центра денежных средств не предоставляет Удостоверяющий Центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности.

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

4.1.12. Без уведомления прекратить действие Сертификата в случае невыполнения Владелец сертификата обязанностей, указанных в подразделе 5.3 настоящего Порядка, а также в случае появления достоверных сведений о том, что документы, представленные в соответствии с подразделом 5.1 настоящего Порядка, не являются подлинными или не подтверждают достоверность всей информации, включённой в данный Сертификат, и/или в случае, если услуга по созданию и выдаче данного Сертификата не оплачена в надлежащем порядке.

4.1.13. Прекратить действие Сертификата в случае получения Удостоверяющим центром подтверждения факта смерти Владельца сертификата.

4.1.14. Использовать представленные Заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия Сертификата, аутентификационной информации в соответствии с подразделом 7.2.1 настоящего Порядка и иной информации.

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

4.2. Обязанности Удостоверяющего центра

4.2.1. 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.

4.2.2. 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.

4.2.3. Обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.

4.2.4. 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.

4.2.5. 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.

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

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

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

4.2.9. Проверку достоверности документов и сведений, представленных Заявителем осуществлять одним из следующих способов:

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

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

– с использованием единой системы идентификации и аутентификации.

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

4.2.11. При выдаче Сертификата установить личность Заявителя, обратившегося за получением Сертификата.

4.2.12. 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.

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

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

4.2.15. Осуществлять формирование и ведение Реестра сертификатов.

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

4.2.17. В случае принятия решения о прекращении своей деятельности без передачи функции Удостоверяющего центра другим лицам сообщить об этом на сайте <https://sovcombank.ru/> и в уполномоченный федеральный орган не позднее, чем за 1 (Один) месяц до даты прекращения своей деятельности, и передать в уполномоченный федеральный орган Реестр сертификатов.

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

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

4.2.20. Исполнять прочие обязанности, предусмотренные Федеральным законом №63-ФЗ,

другими Федеральными законами и иными нормативными актами.

4.3. Ответственность Удостоверяющего центра

4.3.1. Удостоверяющий центр несет гражданско-правовую и (или) административную ответственность, а его работники несут гражданско-правовую и (или) административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом №63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

4.3.2. 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.

4.3.3. 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.

4.3.4. 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.

5. ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СЕРТИФИКАТА

5.1. Обязанности Заявителя

5.1.1. Предъявить документы Заявителя в соответствии с подразделом 6.2.4 настоящего Порядка.

5.1.2. Обеспечить личную явку в Центр выдачи Заявителя.

5.1.3. Представить в Удостоверяющий центр документы, предусмотренные Федеральным законом №63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем, и иные необходимые для создания Сертификата документы.

5.1.4. Заявитель обязуется в течение 30 календарных дней с момента поступления на счет Удостоверяющего центра денежных средств, предоставить в Удостоверяющий Центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности. В случае неисполнения Заявителем данного обязательства, Удостоверяющий центр в течение 30 календарных дней вправе в одностороннем порядке оформить возврат денежных средств на реквизиты счета с которого была произведена оплата, дополнительно отправив информацию о возврате одним из способов, указанных в Регламенте электронного документооборота в Информационной системе (далее – Регламент ИС), опубликованному на сайте в сети Интернет по адресу <https://fintender.ru/service/>.

5.2. Права Владельца сертификата

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

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

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

5.3. Обязанности Владельца сертификата

5.3.1. Все обязанности, предусмотренные подразделом 6.2 настоящего Порядка.

5.3.2. Обеспечить выполнение Правил по обеспечению безопасности на рабочем месте, опубликованных на сайте <https://sovcombank.ru/>.

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

5.3.4. 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.

5.3.5. 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.

5.3.6. При выдаче Сертификата под расписку ознакомиться с информацией, включаемой в Сертификат.

5.3.7. 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 о Средствах электронной подписи, использовавшихся для создания Ключа ЭП и Ключа проверки ЭП, и о Средствах электронной подписи, с которыми будет использоваться Сертификат. При создании Ключа ЭП и запроса на Сертификат должен использоваться алгоритм ГОСТ Р 34.10-2012 с длиной ключа 256 бит.

6. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

6.1. Права Участников электронного взаимодействия

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

6.1.2. Получить Сертификат Удостоверяющего центра.

6.1.3. Получить Сертификат, находящийся в Реестре сертификатов Удостоверяющего центра.

6.1.4. Применять Сертификат для проверки ЭП в электронных документах.

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

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

6.2. Обязанности Участников электронного взаимодействия

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

6.2.2. 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.

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

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

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

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

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

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

Создание Ключей электронной подписи осуществляется Заявителем самостоятельно либо на своем рабочем месте, либо в Центре выдачи.

Заявитель самостоятельно создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный №6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. №173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный №17350);

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

7.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра. Порядок информирования Владельцев сертификатов об осуществлении такой смены.

Плановая смена Ключей Удостоверяющего центра (Ключа ЭП и соответствующего ему Ключа проверки ЭП) выполняется не ранее, чем через 1 (Один) год и не позднее, чем через 1 (Один) год и 3 (Три) месяца после начала действия соответствующего Ключа. Основанием для плановой смены Ключей Удостоверяющего центра является истечение соответствующего срока.

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

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

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

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: <https://sovcombank.ru/>. Для доверенного получения нового сертификата Удостоверяющего центра Владельцы сертификатов обращаются в Центры выдачи Удостоверяющего центра.

7.1.3. 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 7.1.2 настоящего Порядка.

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

После выполнения процедуры внеплановой смены Ключа электронной подписи Удостоверяющего центра прекращается действие Сертификата Ключа проверки электронной подписи, Ключ электронной подписи которого подвергнут процедуре внеплановой смены.

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

Удостоверяющий центр информирует Владельцев сертификатов, которые прекращают свое действие, о факте внеплановой смены Ключей Удостоверяющего центра посредством уведомления на электронную почту, указанную в сертификате и размещения информации на официальном сайте Удостоверяющего центра: <https://sovcombank.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 7.2 настоящего Порядка.

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

7.1.4. 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 Заявления на выдачу Сертификата.

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

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

7.2. Процедура создания и выдачи Сертификатов

7.2.1. Порядок подачи Заявления на выдачу Сертификата.

7.2.1.1. Заявитель самостоятельно регистрируется в ИС, где может подготовить Заявление на выдачу Сертификата в электронном виде, а также передать в Удостоверяющий центр электронные копии документов, при условии подтверждения их соответствия оригиналам в Центре выдачи.

7.2.1.2. Заявитель подписывает Заявление на выдачу Сертификата собственноручно при личном обращении в Центр выдачи.

Создание и выдача Сертификата осуществляется Удостоверяющим центром на основании Заявления на выдачу Сертификата учетом полученного акцепта уведомления о создании Сертификата.

7.2.2. Требование к Заявлению на выдачу Сертификата.

Заявление на выдачу Сертификата может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручно, так и в электронном виде, подписанное КЭП. С образцом Заявления на выдачу Сертификата можно ознакомиться по адресу <https://sovcombank.ru/>. Данный пример носит исключительно ознакомительный характер, за получением актуальной формой Заявления на выдачу Сертификата Заявитель обращается в Центр выдачи (адреса Центров выдачи публикуются на сайте <https://sovcombank.ru/>). Актуальную форму Заявления на выдачу Сертификата Удостоверяющий центр определяет самостоятельно, исходя из цели создания Сертификата. Удостоверяющий центр по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия. Собственноручное подписание Заявления на выдачу Сертификата на бумажном носителе производится чернилами (пастой) синего цвета. Использование факсимиле (клише подписи) на Заявлении на выдачу Сертификата не допускается.

Удостоверяющий центр принимает Заявление на выдачу Сертификата в электронном виде, если Заявитель его подписывает КЭП, Сертификатом ключа проверки которой является действующим на момент подписания, выданным удостоверяющим центром, аккредитованным в соответствии с Федеральным законом №63-ФЗ.

7.2.3. Порядок идентификации Заявителя.

Идентификация Заявителя осуществляется:

7.2.3.1. При личном обращении при предъявлении следующих документов:

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.

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

7.2.3.2. Без его личного присутствия:

- с использованием усиленной квалифицированной электронной подписи при наличии действующего квалифицированного сертификата;
- путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 8 ноября 2019 г. №1427 «О проведении эксперимента по совершенствованию применения технологии электронной подписи»;
- путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

7.2.4. 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.

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

Заявитель представляет в Удостоверяющий центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения Заявителя, а также документы, на основании которых Удостоверяющим центром вносятся сведения в Сертификат, такие как: ФИО адрес прописки, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, и иные данные. Если для подтверждения каких-либо сведений, вносимых в Сертификат, действующим законодательством или настоящим Порядком установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти (например, налоговыми органами). При необходимости копии с документов могут быть сняты и заверены Доверенным лицом Удостоверяющего центра.

Нотариально заверенные копии документов 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 или дипломатическими (консульскими) органами.

7.2.5. Порядок проверки достоверности документов и сведений, предоставленных Заявителем.

Для заполнения Сертификата в соответствии с частью 2 статьи 17 Федерального закона №63-ФЗ Удостоверяющий центр запрашивает и получает из государственных информационных

ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона №63-ФЗ. В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в Сертификат, и Удостоверяющим центром установлена личность Заявителя, Удостоверяющий центр осуществляет процедуру создания и выдачи Заявителю Сертификата. В противном случае Удостоверяющий центр отказывает Заявителю в выдаче Сертификата.

7.2.6. Порядок создания Сертификата.

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

- факт принадлежности документов предоставившему их лицу;
- факт соответствия сведений, указанных в заявлении на выдачу Сертификата, представленным документам и, в необходимых случаях в соответствии с Федеральным законом №63-ФЗ, информации, полученной из государственных реестров;
- факт отсутствия явных признаков подделки документов.

В случае внесения в Сертификат персональных данных физического лица, Заявитель предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных». Текст согласия включен в Заявление на 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.

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

7.2.7. Порядок выдачи Сертификата.

При получении квалифицированного сертификата Заявителем он должен быть ознакомлен аккредитованным 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, 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.

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

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

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

Срочное создание и выдача Сертификата производится в соответствии с условиями Тарифов на услуги УЦ Удостоверяющего центра.

7.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов.

7.3.1. 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, которое составлено в свободной форме. К заявлению прикладывается электронный документ и ЭП, подтверждение которой производится.

7.3.2. 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.

7.3.3. 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.

7.4. Процедуры, осуществляемые при прекращении действия и аннулировании Сертификата

7.4.1. 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 на прекращение Сертификата Владельца сертификата;
- в случае увольнения работника Удостоверяющего центра, которому был выдан Сертификат для выполнения трудовых обязанностей;
 - в случае расторжения договора гражданско-правового характера, предметом которого является оказание услуг или выполнение работ, если Сертификат был выдан для выполнения обязанностей по такому договору;
- по решению Удостоверяющего центра в случаях, предусмотренных пунктами 4.1.12, 4.1.13 настоящего 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.

7.4.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) Сертификата.

Заявление на прекращение сертификата может подаваться в УЦ в бумажной форме при личном прибытии Владельца сертификата в УЦ либо почтовой или курьерской службой, а также в форме электронного документа, подписанного усиленной КЭП Владельца сертификата, в том числе с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)».

Подтверждения полномочий Владельца сертификата осуществляется на основании предоставляемых Заявителем документов. Заявление на прекращение Сертификата должно содержать:

- фамилию, имя, отчество (если имеется) владельца квалифицированного сертификата;
- страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица;
- серийный номер квалифицированного Сертификата;
- даты начала и окончания действия, квалифицированного Сертификата;
- причины прекращения действия квалифицированного сертификата;
- наименование аккредитованного удостоверяющего центра, выдавшего квалифицированный Сертификат.

В случае направления Заявителем Заявления на прекращение Сертификата с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» принятое по заявлению решение удостоверяющего центра в форме электронного документа, подписанного усиленной КЭП УЦ направляется в указанную государственную информационную систему для размещения решения после проведения проверки действительности усиленной КЭП УЦ, которой решение подписано, и подтверждения ее действительности в личном кабинете Заявителя. В случае принятия положительного решения по заявлению УЦ направляет информацию в федеральную государственную информационную систему «Единый портал государственных и муниципальных услуг (функций)» о прекращении действия квалифицированного сертификата после внесения соответствующей информации в Реестр сертификатов. Направление указанных решений и информации осуществляется посредством единой системы межведомственного электронного взаимодействия».

7.4.3. Порядок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов.

Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в Реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона №63-ФЗ, или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие Сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

7.5. Порядок ведения Реестра сертификатов.

7.5.1. 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.

7.5.2. 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 Сертификата или наступления иного события, предусмотренного пунктом 7.4.1 настоящего Порядка.

7.6. Порядок технического обслуживания Реестра сертификатов.

7.6.1. 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.

7.6.2. 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://sovcombank.ru/>.

8. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

8.1. 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 квалифицированной электронной подписи и средств квалифицированной электронной подписи, согласно Приложению №1 к Заявлению на выдачу Сертификата, которое выдается Заявителю одновременно с выдачей Сертификата, а также путем размещения его на официальном сайте УЦ: <https://sovcombank.ru/>.

8.2. Выдача по обращению Заявителя средств электронной подписи.

Выдаваемые средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона №63-ФЗ 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.

8.3. 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.

8.4. 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://sovcombank.ru/>, в любое время, за исключением периодов технического обслуживания Реестра сертификатов.

8.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

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

В Удостоверяющем центре Ключ электронной подписи создается Заявителем на

автоматизированном рабочем месте, аттестованном на соответствие требованиям по безопасности информации, размещенном в помещении Центра выдачи, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель. После окончания процедуры создания Ключа электронной подписи Заявитель забирает ключевой носитель с записанным на нем Ключом электронной подписи.

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

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

8.6. Осуществление регистрации квалифицированного Сертификата в единой системе идентификации и аутентификации.

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

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

При выдаче сертификата Удостоверяющий центр по желанию лица, которому выдан Сертификат, безвозмездно осуществляет регистрацию Владельца сертификата в ЕСИА.

8.8. Предоставление доступа к Реестру сертификатов.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к Реестру Сертификатов.

Для получения доступа к Реестру сертификатов заинтересованное лицо заполняет форму запроса на сайте Удостоверяющего центра. Информация предоставляется заинтересованному лицу в форме электронного сообщения на указанный в форме запроса адрес электронной почты.

9. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ И СЕРТИФИКАТОВ

9.1. 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.

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

9.3. 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.

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