Банк ВТБ
(публичное акционерное общество)

ПОРЯДОК
РЕАЛИЗАЦИИ ФУНКЦИЙ АККРЕДИТОВАННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ИСПОЛНЕНИЯ ЕГО ОБЯЗАННОСТЕЙ

Версия 1.2

2023

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Термины и определения

1.1.1. Аккредитация Удостоверяющего центра – признание Удостоверяющего центра уполномоченным федеральным органом соответствующим требованиям Федерального закона «Об электронной подписи».

1.1.2. Владелец сертификата ключа проверки электронной подписи – лицо, которому удостоверяющим центром выдан сертификат ключа проверки электронной подписи.

1.1.3. Единый портал - федеральная государственная информационная система "Единый портал государственных и муниципальных услуг (функций)" в соответствии с Положением о федеральной государственной информационной системе "Единый портал государственных и муниципальных услуг (функций)", утвержденное постановлением Правительства Российской Федерации от 24 октября 2011 г. N 861.

1.1.4. Заявитель – физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, обращающиеся с соответствующим заявлением на создание и выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

1.1.5. Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом.

1.1.6. Ключ проверки электронной подписи (ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи

1.1.7. Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи.

1.1.8. Компрометация ключа ЭП – утрата доверия к тому, что используемый ключ ЭП обеспечивает безопасность информации; наличие обстоятельств, при которых возможно несанкционированное использование ключа ЭП неуполномоченными лицами.

1.1.9. Сертификат ключа проверки электронной подписи (сертификат) – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

1.1.10. Средства электронной подписи (средства ЭП) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

1.1.11. Удостоверяющий центр – юридическое лицо Банк ВТБ (публичное акционерное общество) (далее - Банк ВТБ (ПАО), осуществляющее функции по созданию и выдаче квалифицированных сертификатов, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».

1.1.12. Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

1.1.13. Федеральный закон «Об электронной подписи» – Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

1.1.14. Электронная подпись (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.

1.1.15. 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.

1.2. Предмет регулирования Порядка

1.2.1. Настоящий Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее – Порядок) определяет условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра.

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

1.2.3. Присоединение к настоящему Порядку осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр Заявление о присоединении к Порядку по форме, приведенной в Приложении **1** к настоящему Порядку.

1.2.4. Любое заинтересованное лицо может ознакомиться с Порядком на сайте Удостоверяющего центра по адресу https://www.gostpki.vtb.ru/.

1.2.5. Владелец сертификата имеет право прекратить взаимодействие с Удостоверяющим центром в рамках Порядка, направив в Удостоверяющий центр заявление о прекращении действия выданного ему сертификата по форме Приложения 3 к настоящему Порядку.

1.2.6. Внесение изменений (дополнений) в Порядок (включая приложения к нему) производится Удостоверяющим центром в одностороннем порядке. Уведомление участников информационного взаимодействия о внесении изменений (дополнений) в Порядок осуществляется Удостоверяющим центром путем публикации на сайте по адресу https://www.gostpki.vtb.ru/.

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

1.3. Сведения об Удостоверяющем центре

1.3.1. Полное наименование Удостоверяющего центра: Банк ВТБ (Публичное акционерное общество).

1.3.2. Краткое наименование Удостоверяющего центра: Банк ВТБ (ПАО).

1.3.3. Юридический адрес: 191144, г. Санкт-Петербург, переулок Дегтярный, дом 11, литер А.

1.3.4. Место нахождения Удостоверяющего центра: 109147, г. Москва, ул. Воронцовская, д. 43, стр. 1, Банк ВТБ (ПАО).

1.3.5. Основной государственный регистрационный номер (ОГРН): 1027739609391.

1.3.6. Идентификационный номер налогоплательщика (ИНН): 7702070139.

1.3.7. Удостоверяющий центр осуществляет функции по созданию и выдаче сертификатов ключей проверки электронных подписей и иные функции, предусмотренные Федеральным законом «Об электронной подписи» и действует на основании:

- аккредитации Удостоверяющего центра Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации;

- лицензии № 78/1314/Н от 24.05.2021, выданной Банку ВТБ (ПАО) Управлением ФСБ Российской Федерации по городу Санкт-Петербургу и Ленинградской области, на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

1.3.8. График работы Удостоверяющего центра: по рабочим дням: понедельник-четверг с 09:00 до 18:00, пятница с 09:00 до 16:45 (время Московское). В выходные и праздничные дни Удостоверяющий центр не работает.

1.3.9. Удостоверяющий центр осуществляет прием от Заявителя заявок, заявлений, документов и сведений по месту нахождения Удостоверяющего центра по рабочим дням: понедельник-четверг с 09:00 до 18:00, пятница с 09:00 до 16:45 (время Московское).

1.3.10. Техническая поддержка Заявителя осуществляется Удостоверяющим центром по рабочим дням: понедельник-четверг с 09:00 до 18:00, пятница с 09:00 до 16:45 (время Московское) по телефону или по адресу электронной почты в сети Интернет pki@vtb.ru.

1.4. Порядок информирования о предоставлении услуг Удостоверяющего центра

1.4.1. Удостоверяющий центр осуществляет информирование Заявителя о предоставлении услуг Удостоверяющего центра по телефонам, по электронной почте, через Web-сайт Удостоверяющего центра.

1.4.2. Контактные телефоны Удостоверяющего центра: 8-800-200-77-99, +7 (495) 739-77-99 (единая справочная служба).

1.4.3. Адрес Web-сайта Удостоверяющего центра: https://www.gostpki.vtb.ru/,

1.4.4. Адрес электронной почты Удостоверяющего центра: pki@vtb.ru.

1.4.5. Удостоверяющий центр информирует Заявителя о порядке использования электронных подписей и средств ЭП при заключении с ним соглашения, в электронной форме и по телефону.

1.4.6. Удостоверяющий центр по письменному запросу Заявителя предоставляет ему:

- копии документов, на основании которых Удостоверяющий центр осуществляет свою деятельность, заверенные подписью уполномоченного лица Удостоверяющего центра и оттиском печати Удостоверяющего центра;
- копию действующего Порядка на бумажном носителе, заверенную подписью уполномоченного лица Удостоверяющего центра и оттиском печати Удостоверяющего центра.

1.5. Стоимость услуг Удостоверяющего центра.

1.5.1. Оплата услуг Удостоверяющего центра производится в соответствии с тарифами Банка ВТБ (ПАО).

1.5.2. Информирование о тарифах, сроках и порядке расчетов за оказание услуг осуществляется путем публикации данной информации на сайте по адресу https://www.vtb.ru/.

2. Перечень реализуемых Удостоверяющим центром функций

2.1. Удостоверяющий центр реализует следующие функции:

2.1.1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты заявителям при условии идентификации заявителя. 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 информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

2.1.2. 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.

2.1.3. Устанавливает сроки действия сертификатов ключей проверки электронных подписей.

2.1.4. Аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей.

2.1.5. 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;

2.1.6. 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.

2.1.7. Создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей.

2.1.8. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов.

2.1.9. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.

2.1.10. Обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет".

2.1.11. Осуществляет иную связанную с использованием электронной подписи деятельность.

3. Права и обязанности Удостоверяющего центра

3.1. Права Удостоверяющего центра

Удостоверяющий центр имеет право:

3.1.1. Отказать Заявителю в выдаче квалифицированного сертификата в случае невыполнения Заявителем обязанностей, установленных Федеральным законом «Об электронной подписи» и принимаемыми в соответствии с ним нормативными правовыми актами.

3.1.2. Отказать владельцу сертификата в прекращении действия сертификата в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям.

3.1.3. аннулировать сертификат ключа проверки электронной подписи в случаях, указанных в части 6.1 статьи 14 Федерального закона «Об электронной подписи».

3.1.4. Третьи лица на основании заключенного с удостоверяющим центром соглашения или на основании нормативного правового акта Российской Федерации наделяются полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра (далее - доверенные лица). При совершении порученных удостоверяющим центром действий доверенное лицо обязано идентифицировать заявителя при его личном присутствии.

3.1.5. Удостоверяющий центр не вправе наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени Удостоверяющего центра.

3.1.6. Выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе.

3.2. Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

3.2.1. Информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

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

3.2.3. 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.

3.2.4. Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.

3.2.5. 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.

3.2.6. 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.

3.2.7. 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.

3.2.8. Направлять в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

3.2.9. При выдаче квалифицированного сертификата:

- идентифицировать заявителя, обратившееся к нему за получением квалифицированного сертификата, в соответствии с требованиями статьи 18 Федерального закона «Об электронной подписи»;

- по желанию владельца квалифицированного сертификата безвозмездно осуществлять его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии;

- предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

3.2.10. Хранить следующую информацию:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

3.2.11. удостоверяющий центр должен хранить информацию, указанную в пункте 3.2.10, в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.2.12. Использовать для подписания от своего имени квалифицированных сертификатов квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

3.2.13. Не допускать использования квалифицированной электронной подписи, основанной на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

3.2.14. Осуществлять ознакомление Заявителя под расписку при получении им квалифицированного сертификата с информацией, содержащийся в квалифицированном сертификате.

3.2.15. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр:

- 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 этим аккредитованным удостоверяющим центром квалифицированных сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

3.2.16. Выполнять настоящий Порядок в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с Федеральным законом «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи».

3.2.17. Выдать владельцу квалифицированного сертификата одновременно с выдачей квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

3.2.18. Удостоверяющий центр на безвозмездной основе обеспечивает физических лиц шифровальными (криптографическими) средствами, указанными в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", для проведения идентификации физических лиц в аккредитованном удостоверяющем центре на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети "Интернет".

3.2.19. Исполнять иные обязанности, устанавливаемыми Федеральным законом «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними нормативными актами.

3.3. Удостоверяющему центру запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

4. Права и обязанности Заявителя

4.1. Права Заявителя

Заявитель имеет право:

4.1.1. Обратиться в Удостоверяющий центр с целью создания и выдачи ему квалифицированного сертификата.

4.1.2. Обратиться в Удостоверяющий центр с целью прекращения действия выданного ему квалифицированного сертификата.

4.2. Обязанности Заявителя

Заявитель обязан:

4.2.1. Обеспечивать конфиденциальность ключа ЭП, в частности не допускать использование принадлежащего ему ключа ЭП без своего согласия.

4.2.2. Уведомлять Удостоверяющий центр, выдавший квалифицированный сертификат, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

4.2.3. Не использовать ключ ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

4.2.4. Применять средства ЭП в соответствии с положениями эксплуатационной документации на соответствующее средство ЭП.

4.2.5. Использовать для создания и проверки электронных подписей, создания ключа ЭП и ключа проверки ЭП средства ЭП, имеющие подтверждение соответствия требованиям, установленным Федеральным законом «Об электронной подписи».

4.2.6. Предоставить Удостоверяющему центру документы и сведения, предусмотренные настоящим Порядком и законодательством Российской Федерации, регулирующим отношения в области использования электронных подписей.

5. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром, в том числе требования к документам, предоставляемым в удостоверяющий центр в рамках предоставления услуг

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

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

5.1.1.1. Создание ключа ЭП и ключа проверки ЭП может производиться Удостоверяющим центром или самостоятельно Заявителем:

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

5.1.1.2. Ключ ЭП и ключ проверки ЭП, 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 и с соблюдением требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя.

5.1.1.3. Одновременно с созданием ключей ЭП производится формирование файла с запросом на сертификат ключа проверки ЭП.

5.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, а также порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата Удостоверяющего центра.

5.1.2.1. Плановая смена ключей ЭП выполняется в период действия ключа ЭП Удостоверяющего центра.

5.1.2.2. Плановая смена ключей ЭП Удостоверяющего центра производится по следующим основаниям:

- истечение срока использования ключа ЭП;
- переход на использование новых стандартов ЭП в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования электронной подписи или безопасности.

5.1.2.3. Процедура плановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;

- Удостоверяющий центр получает квалифицированный сертификат Удостоверяющего центра в уполномоченном органе исполнительной власти в установленном им порядке.

5.1.2.4. Порядок, дата и время перехода на новый сертификат Удостоверяющего центра содержатся в уведомлении о смене ключей ЭП Удостоверяющего центра и о переходе на новый сертификат Удостоверяющего центра на сайте Удостоверяющего центра по адресу: https://www.gostpki.vtb.ru/. Доверенным способом получения нового квалифицированного сертификата Удостоверяющего центра является его публикация на официальном сайте Удостоверяющего центра по адресу https://www.gostpki.vtb.ru/, доступная для скачивания.

5.1.2.5. Старые ключи ЭП Удостоверяющий центр использует в течение срока действия данных ключей ЭП для подписания списка отозванных сертификатов, выпущенных Удостоверяющим центром в течение срока действия данных ключей ЭП.

5.1.2.6. Плановая смена ключа ЭП Удостоверяющего центра выполняется не позднее, чем за 1 месяц до окончания срока действия текущего ключа ЭП Удостоверяющего центра.

5.1.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности.

5.1.3.1. В случае нарушения конфиденциальности ключа ЭП Удостоверяющего центра или угрозы нарушения конфиденциальности такого ключа ЭП осуществляется внеплановая смена ключа ЭП и ключа проверки ЭП Удостоверяющего центра.

5.1.3.2. К событиям, указывающих на нарушение конфиденциальности (компрометацию) ключа ЭП Удостоверяющего центра, относятся следующие:
- ознакомление неуполномоченного лица (лиц) с ключом ЭП;
- утрата ключевого носителя с ключом ЭП;
- утрата ключевого носителя с ключом ЭП с последующим обнаружением;
- нарушение правил хранения ключевых носителей;
- нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных для хранения ключевых носителей;
- утрата ключей от сейфов (шкафов, хранилищ), предназначенных для хранения ключевых носителей;
- утрата ключей от сейфов (шкафов, хранилищ), предназначенных для хранения ключевых носителей с последующим обнаружением;
- случаи, для которых невозможно достоверно установить, что произошло с ключевыми носителями (в том числе обстоятельства, при которых ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

5.1.3.3. К актуальным видам угроз нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра относятся:
- угроза несанкционированного доступа к защищаемой информации, связанного с неправомерными действиями нарушителей (несанкционированный доступ в помещения, в которых располагаются программные средства Удостоверяющего центра, подозрение на перехват ключевой информации по техническим каналам утечки, подозрение на кражу носителя, на котором хранится ключ электронной подписи Удостоверяющего центра, и т.д.);
- непреднамеренные (неумышленные) действия сотрудников Удостоверяющего центра (заражение программных средств Удостоверяющего центра вредоносным программным обеспечением, нарушение правил хранения и эксплуатации ключей электронной подписи Удостоверяющего центра и т.д.).

5.1.3.4. В случае нарушения конфиденциальности ключа ЭП Удостоверяющего центра или наличия угрозы нарушения конфиденциальности данного ключа ЭП выполняется аннулирование (отзыв) сертификата, соответствующего данному ключу ЭП Удостоверяющего центра, и осуществляется внеплановая смена ключа ЭП и ключа проверки ЭП Удостоверяющего центра.

5.1.3.5. Процедура внеплановой смены ключей ЭП Удостоверяющего центра осуществляется в срок не более 24 часов с момента выявления факта компрометации или угрозы компрометации ключей ЭП Удостоверяющего центра

5.1.3.6. Процедура внеплановой смены мена ключа ЭП и ключа проверки ЭП Удостоверяющего центра производится в порядке, установленном для плановой смены ключа ЭП Удостоверяющего центра, в соответствии с п. 5.1.2.3 настоящего Порядка.

5.1.3.7. Одновременно с прекращением действия ключа ЭП Удостоверяющего центра в случае нарушения конфиденциальности или наличия угрозы нарушения конфиденциальности данного ключа ЭП прекращается действие всех квалифицированных сертификатов, созданных с использованием данного ключа ЭП, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

5.1.3.8. Информация об отзыве действующего сертификата Удостоверяющего центра, о сроках и порядке получения нового сертификата Удостоверяющего центра, размещается на сайте Удостоверяющего центра по адресу https://www.gostpki.vtb.ru/.

5.1.3.9. Доверенным способом получения нового квалифицированного сертификата Удостоверяющего центра является его публикуется на официальном сайте Удостоверяющего центра по адресу: https://www.gostpki.vtb.ru/, доступная для скачивания.

5.1.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца квалифицированного сертификата

5.1.4.1. Смена ключа ЭП владельца квалифицированного сертификата осуществляется в следующих случаях:

- в связи истечением установленного срока его действия;
- на основании Заявления о прекращении действия квалифицированного сертификата по форме Приложения **3** к настоящему Порядку в соответствии с п. 5.4 настоящего Порядка в виде документа на бумажном носителе или в форме электронного документа;
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и владельцем сертификата ключа проверки ЭП;
- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в данном сертификате;
- установлено, что содержащийся в данном сертификате ключ проверки ЭП уже содержится в ином ранее созданном сертификате ключа проверки ЭП;
- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки ЭП содержит недостоверную информацию.

5.1.4.2. При смене ключа ЭП Заявитель в соответствии с п. 5.1.1.1 создает ключ ЭП самостоятельно или обращается в Удостоверяющий центр за получением услуги создания ключа ЭП и оформляет Заявление на создание и выдачу квалифицированного сертификата в соответствии с требованиями раздела 5.2 настоящего Порядка.

5.1.4.3. Выдача квалифицированного сертификата производится в соответствии с п. 5.2.7 настоящего Порядка.

5.2. Процедура создания и выдачи квалифицированных сертификатов

5.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов.

5.2.1.1. Заявление на создание и выдачу квалифицированного сертификата подается лицами, присоединившимися к Порядку в соответствии с п. 1.2.3 настоящего Порядка.

5.2.1.2. Заявление на создание и выдачу квалифицированного сертификата может быть подано как в форме документа, на бумажном носителе и заверенного собственноручной подписью владельца сертификата, при личном прибытии по месту нахождения Удостоверяющего центра, так и в форме электронного документа, подписанного усиленной

квалифицированной ЭП владельца квалифицированного сертификата, направленного в Удостоверяющий центр по электронным каналам связи. При этом в случае, если смена ключа ЭП владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, Заявление должно быть подписано иной усиленной квалифицированной ЭП владельца квалифицированного сертификата.

5.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

5.2.2.1. 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, 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) и информации из государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных" (далее - единая биометрическая система).

5.2.2.2. Заявление на создание и выдачу квалифицированного сертификата может включать указание на создание ключа ЭП владельца Удостоверяющим центром в соответствии с п. 5.1.1 настоящего Порядка.

5.2.2.3. Форма Заявления на создание и выдачу квалифицированного сертификата приведена в Приложении **2** к настоящему Порядку.

5.2.3. Порядок идентификации заявителя.

5.2.3.1. Идентификация гражданина Российской Федерации осуществляется:

1) при его личном присутствии по основному документу, удостоверяющему личность;

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. N 1427 "О проведении эксперимента по совершенствованию применения технологии электронной подписи" (Собрание законодательства Российской Федерации, 2019, N 46, ст. 6493);

- путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2020, N 14, ст. 2035).

5.2.3.2. Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

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

5.2.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата:

5.2.4.1. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя, в соответствии с частью 2 статьи 18 Федерального закона «Об электронной подписи» изложен в пункте 5.2.7.3 настоящего Порядка.

5.2.4.2. 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.

5.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем:

5.2.5.1. 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».

5.2.5.2. В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и Удостоверяющий центр идентифицировал заявителя - физическое лицо, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В ином случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

5.2.6. Порядок создания квалифицированного сертификата

5.2.6.1. Создание квалицированного сертификата осуществляется на основании запроса, полученного в порядке, установленном разделом 5.1.1 настоящего Порядка.

5.2.6.2. Структура и форма квалифицированного сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ России от 27.12.2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

5.2.6.3. При создании квалифицированного сертификата Удостоверяющий центр проверяет уникальность ключей проверки ЭП. В случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки ЭП, указанного Заявителем, Удостоверяющий центр отказывает Заявителю в создании квалифицированного сертификата.

5.2.7. Порядок выдачи квалифицированного сертификата

5.2.7.1. При выдаче квалифицированного сертификата Удостоверяющий центр обязан:

1) в порядке, установленном Федеральным законом «Об электронной подписи», идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата 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 Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации. Устанавливаются:

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

2) в установленном пунктом 5.2.3 порядке идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, 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 посредством идентификации заявителя - 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 в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

3) предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

5.2.7.2. Подтверждение достоверности сведений, перечисленных в подпункте 1 пункта 5.2.7.1, осуществляется 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.

5.2.7.3. При обращении в аккредитованный удостоверяющий центр заявитель представляет следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

1) основной документ, удостоверяющий личность;

2) страховой номер индивидуального лицевого счета заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица;

5.2.7.4. Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в подпунктах 2 - 3 пункта 5.2.7.3 настоящего Порядка.

5.2.7.5. Аккредитованный удостоверяющий центр должен с использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных заявителем в соответствии с пунктами 5.2.7.3 и 5.2.7.4 настоящего Порядка.

5.2.7.6. В случае, если полученные в соответствии с пунктом 5.2.7.5 настоящего Порядка сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и аккредитованным удостоверяющим центром идентифицирован заявитель, аккредитованный 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», аккредитованный удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

5.2.7.7. 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 - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи (утвержденными Постановлением Правительства РФ от 25.01.2013 № 33) 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.

5.2.7.8. Квалифицированный сертификат выдается аккредитованным удостоверяющим центром на безвозмездной основе или за установленную удостоверяющим центром плату в соответствии с пунктом 1.5 настоящего Порядка при условии, что размер такой платы не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

5.2.7.9. Аккредитованный удостоверяющий центр одновременно с выдачей квалифицированного сертификата предоставляет владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной

электронной подписи и средств квалифицированной электронной подписи в форме Приложения **4** к настоящему Порядку.

5.2.7.10. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг утверждены постановлением Правительства Российской Федерации от 28.12.2020 № 2309. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

5.2.7.11. Удостоверяющий центр создает квалифицированный сертификат в электронном виде, а также два экземпляра квалифицированного сертификата на бумажном носителе. При получении квалифицированного сертификата владельцем квалифицированного сертификата данное лицо проводит ознакомление с информацией, содержащейся в сертификате. Оба экземпляра квалифицированного сертификата на бумажном носителе заверяются собственноручной подписью Заявителя, а также собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра. После оформления квалифицированного сертификата на бумажном носителе Удостоверяющий центр выдает Заявителю сертификат ключа проверки электронной подписи в электронном виде и один экземпляр квалифицированного сертификата на бумажном носителе. Второй экземпляр квалифицированного сертификата на бумажном носителе хранится в Удостоверяющем центре.

5.2.8. Срок создания и выдачи квалифицированного сертификата, а также условия для срочного создания и выдачи квалифицированного сертификата заявителю.

5.2.8.1. Срок создания и выдачи квалифицированного сертификата заявителю не должен превышать 5 (пяти) рабочих дней с момента получения Удостоверяющим центром соответствующего Заявления.

5.2.8.2. Создание и выдача квалифицированного сертификата Заявителю в срочном порядке Удостоверяющим центром не предусмотрены.

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

5.3.1. По желанию стороны, присоединившейся к Порядку, Удостоверяющий центр выполняет процедуру подтверждения действительности электронной подписи в электронном документе, представленном на экспертизу.

5.3.2. Подтверждение действительности электронной подписи под электронным документом осуществляется Удостоверяющим центром на основании Заявления физического лица, поданного в простой письменной форме.

5.3.3. Заявление на подтверждение действительности подписи под электронным документом подается Заявителем в Удостоверяющий центр лично, почтой с гарантированной доставкой или курьерской службой.

5.3.4. Заявление на подтверждение действительности электронной подписи под электронным документом должно содержать информацию о дате и времени формирования электронной подписи.

5.3.5. Доказательство достоверности даты и времени формирования электронной подписи под электронным документом возлагается на Заявителя.

5.3.6. Обязательным приложением к Заявлению на подтверждение действительности электронной подписи под электронным документом является файл, содержащий подписанный электронной подписью документ формата CMS (PKCS#7).

5.3.7. Срок рассмотрения Заявления на подтверждение действительности электронной подписи под электронным документом не должен превышать 15 (пятнадцати) рабочих дней с момента его поступления в Удостоверяющий центр.

5.3.8. В случае отказа в выполнении экспертных работ по подтверждению действительности электронной подписи под электронным документом Заявителю возвращается Заявление на подтверждение действительности электронной подписи с резолюцией уполномоченного работника Удостоверяющего центра о причине отказа.

5.3.9. В случае принятия положительного решения по Заявлению, Удостоверяющий центр уведомляет Заявителя о принятом решении и проводит работы по проверке действительности электронной подписи под предоставленным электронным документом, включающие процедуру проверки действительности всех квалифицированных сертификатов, включенных в последовательность проверки (от квалифицированного сертификата, соответствующего ключу ЭП, до квалифицированного сертификата Удостоверяющего центра, выданного ему Головным удостоверяющим центром).

5.3.10. Срок оказания услуги по подтверждение действительности электронной подписи под электронным документом составляет 3 (три) рабочих дня с момента принятия положительного решения по заявлению.

5.3.11. После проведения экспертной процедуры Удостоверяющий центр выдает Заявителю заключение о выполненной проверке. Заключение содержит отчет о выполненной проверке действительности электронной подписи, составленный в простой письменной форме и результат проверки подтверждения действительности электронной подписи под электронным документом и заверяется собственноручной подписью заверенный собственноручной подписью уполномоченного работника Удостоверяющего центра и печатью.

5.4. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата

5.4.1. Основания прекращения действия или аннулирования квалифицированного сертификата:

5.4.1.1. Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона «Об электронной подписи»:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца квалифицированного сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и владельцем квалифицированного сертификата.

5.4.1.2. Удостоверяющий центр признает квалифицированный сертификат аннулированным, если:

- не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;
- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;
- вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию.

5.4.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) квалифицированного сертификата.

5.4.2.1. При обращении владельца квалифицированного сертификата с Заявлением о прекращении действия квалифицированного сертификата по форме Приложения **3** к

настоящему Порядку) в виде документа на бумажном носителе или в виде электронного документа, подписанного усиленной квалифицированной подписью, в том числе, начиная с 1 сентября 2024 г[1]., с использованием Единого портала, Удостоверяющий центр подтверждают полномочия владельца квалифицированного сертификата в порядке, предусмотренном пунктом 5.2.3 настоящего Порядка.

5.4.2.2. В случае направления заявителем 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.

5.4.2.3. Удостоверяющий центр вносит в реестр сертификатов информация о прекращении действия (аннулировании) квалифицированного сертификата в течение двенадцати часов с момента наступления обстоятельств, указанных в п, 5.4.1 настоящего Порядка, или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений. Действие квалифицированного сертификата прекращается с момента внесения соответствующей информации в реестр сертификатов.

5.4.2.4. Оповещение владельца квалифицированного сертификата о прекращении действия (аннулировании) квалифицированного сертификата осуществляется путем публикации актуального списка отозванных сертификатов на сайте Удостоверяющего центра по адресу https://www.gostpki.vtb.ru/.

5.5. Порядок ведения реестра квалифицированных сертификатов

5.5.1. Удостоверяющий центр ведет реестр квалифицированных сертификатов в течение всего срока деятельности Удостоверяющего центра.

5.5.2. Реестр квалифицированных сертификатов ведётся в электронном виде.

5.5.3. Реестр квалифицированных сертификатов включает в себя информацию, содержащуюся в выданных Удостоверяющим центром квалифицированных сертификатах, информацию о датах прекращения действия (аннулирования) сертификатов ключей проверки электронных подписей, а также об основаниях прекращения действия (аннулирования).

5.5.4. Информация о выпущенных Удостоверяющим центром квалифицированных сертификатах вносится в реестр сертификатов одновременно с их созданием.

5.5.5. Внесение в реестр сертификатов сведений о прекращении действия (аннулировании) сертификатов осуществляется в срок, предусмотренный п. 5.4.2.3 настоящего Порядка.

5.5.6. Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если иное не установлено нормативными правовыми актами Российской Федерации.

5.6. Порядок технического обслуживания реестра квалифицированных сертификатов

[1] В соответствии с Приказом Минцифры России от 14.07.2023 N 634 "О внесении изменений в Требования к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденные приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13 ноября 2020 г. N 584" (Зарегистрировано в Минюсте России 09.10.2023 N 75507)

5.6.1. Плановые технические работы по обслуживанию реестра квалифицированных сертификатов проводятся Удостоверяющим центром с учетом минимизации перерывов в работе Удостоверяющего центра при использовании квалифицированных сертификатов их владельцами.

5.6.2. Внеплановые технические работы проводятся при появлении такой необходимости в оперативном режиме.

5.6.3. Максимальная продолжительность технического обслуживания реестра квалифицированных сертификатов составляет 24 часа. Время проведения технического обслуживания реестра квалифицированных сертификатов может быть увеличено при наличии объективных оснований и причин.

5.6.4. Удостоверяющий центр информирует участников информационного взаимодействия о проведении технического обслуживания реестра квалифицированных сертификатов путем публикации информационного сообщения на сайте Удостоверяющего центра по адресу https://www.gostpki.vtb.ru/.

6. Порядок исполнения обязанностей Удостоверяющего центра, установленных Федеральным законом «Об электронной подписи» и принимаемыми в соответствии с ним нормативными правовыми актами

6.1. 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.

6.1.1. Удостоверяющий центр осуществляет информирование заявителей об условиях и о порядке использования электронных подписей и средств ЭП, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки в следующем порядке:

- Удостоверяющий центр консультирует владельца квалифицированного сертификата при выдаче ему квалифицированного сертификата;
- одновременно с выдачей квалифицированного сертификата Удостоверяющий центр предоставляет владельцу квалифицированного сертификата руководство по обеспечению безопасности при использовании электронной подписи и средств ЭП.

6.2. Выдача по обращению заявителя средств электронной подписи

6.2.1. Средства ЭП должны в соответствии с частью 4 статьи 6 Федерального закона «Об электронной подписи» обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

6.2.2. Выдача Удостоверяющим центром средств электронной подписи заявителям осуществляется в соответствии с тарифами Банка ВТБ (ПАО) в соответствии с пунктом 1.5. настоящего Порядка.

6.2.3. Условия и порядок использования средств ЭП определяются документацией на средство ЭП и лицензионным соглашением между разработчиком средства электронной подписи и заявителем.

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

6.3.1. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре квалицированных сертификатов, а также ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

6.3.2. Актуальность информации, содержащейся в реестре квалицированных сертификатов, обеспечивается в соответствии с пунктом 5.5 настоящего Порядка.

6.3.3. Защита информации, содержащейся в реестре квалицированных сертификатов от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий обеспечивается путем:

- ограничения доступа в помещения, где размещены аппаратные средства Удостоверяющего центра;
- идентификации, аутентификации и разграничение доступа пользователей и обслуживающего персонала к программным средствам Удостоверяющего центра и защищаемой информации;
- контроля несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- ведения реестра квалифицированных сертификатов в условиях, обеспечивающих предотвращение несанкционированного доступа к нему;
- резервного копирования информации, содержащейся в реестре квалифицированных сертификатов, для предотвращения утраты сведений о сертификатах.

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

6.4.1. Удостоверяющий центр публикует информацию из реестра квалифицированных сертификатов на сайте по адресу https://www.gostpki.vtb.ru/.

6.4.2. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационной сети Интернет к информации из реестра квалифицированных сертификатов в любое время в течение срока деятельности Удостоверяющего центра для определения действительности сертификатов ключей проверки электронной подписи, выданных Удостоверяющим центром владельцам квалифицированных сертификатов, за исключением периодов технического обслуживания реестра квалифицированных сертификатов.

6.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

6.5.1. В целях обеспечения конфиденциальности созданных Удостоверяющим центром ключей ЭП уполномоченным сотрудникам Удостоверяющего центра, выполняющим задачи по созданию и выдаче ключей электронной подписи и сертификатов ключей проверки электронной подписи, запрещается:

- оставлять без контроля вычислительные средства, на которых создаются ключи электронной подписи;
- вносить какие-либо изменения в программное обеспечение, использующееся для создания ключей электронной подписи и сертификатов ключей проверки электронной подписи;
- осуществлять несанкционированное копирование ключей электронной подписи;
- разглашать содержимое носителей ключевой информации и пароль (пин-код), использующийся для защиты создаваемых Удостоверяющим центром ключей электронной подписи, а также передавать ключевые носители лицам, к ним не допущенным;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств криптографической защиты информации;
- записывать на ключевые носители постороннюю информацию;
- оставлять без присмотра ключи ЭП на ключевом носителе.

6.5.2. Уполномоченный сотрудник Удостоверяющего центра несет персональную ответственность за обеспечение конфиденциальности созданных им ключей ЭП.

6.5.3. До создания ключа ЭП и квалифицированного сертификата уполномоченный сотрудник Удостоверяющего центра информирует Заявителя о преимуществах записи ключа ЭП на ключевой носитель в неизвлекаемом режиме и уточняет у Заявителя возможность записи ключа ЭП в таком режиме.

6.5.4. При передаче ключа ЭП и квалифицированного сертификата уполномоченный сотрудник Удостоверяющего центра информирует владельца квалифицированного сертификата о рисках, связанных с использованием электронных подписей, и выдает ему руководство по обеспечению безопасности при использовании электронной подписи и средств ЭП.

6.5.5. Удостоверяющий центр создает и при необходимости уничтожает ключи ЭП 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)».

6.5.6. Создание и уничтожение ключей ЭП осуществляется на автоматизированном рабочем месте Удостоверяющего центра, в отношении которого выполняются требования, установленные постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

6.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации.

6.6.1. Удостоверяющий центр осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации (далее – ЕСИА) в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи».

6.6.2. При выдаче квалифицированного сертификата Удостоверяющий центр направляет в ЕСИА сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате, в том числе:

- уникальный номер квалифицированного сертификата;
- дату начала и окончания действия квалифицированного сертификата;
- наименование Удостоверяющего центра;
- фамилию, имя, отчество владельца квалифицированного сертификата;
- СНИЛС владельца квалифицированного сертификата;
- реквизиты документа, удостоверяющего личность владельца квалифицированного сертификата;
- иные сведения, необходимые для регистрации в ЕСИА.

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

6.7.1. Удостоверяющий центр одновременно с выпуском квалифицированного сертификата безвозмездно регистрирует лицо, обратившееся за получением услуг Удостоверяющего центра, по его желанию, в ЕСИА.

6.7.2. Основанием для регистрации служит официальное обращение в Удостоверяющий центр, содержащее сведения необходимые для регистрации в ЕСИА. Такое обращение в Удостоверяющий центр может подавать только физическое лицо лично.

6.8. 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

6.8.1. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи. Указанная информация предоставляется в форме выписки из реестра сертификатов и направляется обратившемуся лицу как почтовым отправлением, так и с использованием информационно-

телекоммуникационных сетей (по выбору лица, обратившегося за получением информации из реестра квалифицированных сертификатов).

6.8.2. Срок предоставления указанной информации не может превышать 7 (семи) дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно-телекоммуникационных сетей.

6.8.3. Информация о прекращении действия квалифицированного сертификата или об аннулирования квалифицированного сертификата может быть предоставлена любому лицу, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов на сайте Удостоверяющего центра по адресу https://www.gostpki.vtb.ru/.

7. Ответственность сторон

7.1. Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющим центром;
- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом «Об электронной подписи».

7.2. Удостоверяющий центр (работник Удостоверяющего центра) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Порядком.

7.3. За невыполнение или ненадлежащее выполнение обязательств по настоящему Порядку стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного стороне невыполнением или ненадлежащим выполнением обязательств другой стороной.

7.4. Ответственность сторон, не урегулированная положениями настоящего Порядка, регулируется законодательством Российской Федерации.

8. Разрешение споров

8.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и сторона, присоединившаяся к Порядку.

8.2. При рассмотрении спорных вопросов, связанных с настоящим Порядком, Стороны будут руководствоваться действующим законодательством Российской Федерации.

8.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

8.4. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

8.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде.

9. Конфиденциальность информации.

9.1. Типы конфиденциальной информации.

9.1.1. Ключ ЭП, соответствующий квалифицированному сертификату, является конфиденциальной информацией владельца квалифицированного сертификата. Удостоверяющий центр не осуществляет хранение ключей ЭП владельца квалифицированного сертификата.

9.1.2. Персональная информация о владельце квалифицированного сертификата, хранящаяся в Удостоверяющем центре, не являющаяся частью квалифицированного сертификата, считается конфиденциальной.

9.2. Исключительные полномочия Удостоверяющего центра.

9.2.1. Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

10. Форс-мажор.

10.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Порядку, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Порядку.

10.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля сторон) и непредотвратимые при данных условиях обстоятельства, включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения стороной/сторонами своих обязательств по настоящему Порядку.

10.3. В случае возникновения форс-мажорных обстоятельств, срок исполнения сторонами своих обязательств по настоящему Порядку отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

10.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Порядку, должна немедленно известить в письменной форме другую сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

10.5. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

10.6. В случае, если невозможность полного или частичного исполнения сторонами какого-либо обязательства по настоящему Порядку обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой стороной.

11. Список приложений.

11.1. Приложение 1 «Заявление о присоединении к Порядку».

11.2. Приложение 2 «Заявление на создание и выдачу квалифицированного сертификата».

11.3. Приложение 3 «Заявление о прекращении действия квалифицированного сертификата».

11.4. Приложение 4 «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи».

Приложение 1 «Заявление о присоединении к Порядку»
к Порядку реализации функций аккредитованного удостоверяющего центра Банк ВТБ (ПАО) и исполнения его обязанностей

Форма заявления

Заявление о присоединении к Порядку реализации функций аккредитованного удостоверяющего центра Банк ВТБ (ПАО) и исполнения его обязанностей

Я, _____,
(фамилия, имя, отчество)

_____
(серия и номер паспорта)

_____,
(кем и когда выдан)

настоящим заявляю о присоединении к условиям Порядка реализации функций аккредитованного удостоверяющего центра Банка ВТБ (ПАО) и исполнения его обязанностей (далее - Порядок), условия которого определены Удостоверяющим центром Банк ВТБ (ПАО) и опубликованы на сайте Удостоверяющего центра по адресу по адресу https://www.gostpki.vtb.ru/ в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации.

Настоящим подтверждаю, что с Порядком реализации функций аккредитованного удостоверяющего центра Банк ВТБ (ПАО) и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.
Ознакомлен, что все актуальные изменения размещаются на сайте удостоверяющего центра Банка ВТБ (ПАО) по адресу: по адресу https://www.gostpki.vtb.ru/.

Я выражаю свое согласие на осуществление Удостоверяющим центром Банк ВТБ (ПАО) обработки (сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, передачу, обезличивание, блокирование, уничтожение), в том числе автоматизированной, моих персональных данных, указанных в настоящем заявлении, в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Указанные мной персональные данные предоставляются в целях обеспечения взаимодействия с УЦ Банк ВТБ (ПАО) в рамках Порядка и иных продуктов и услуг УЦ Банк ВТБ (ПАО). Согласие предоставляется на весь срок моей жизни. Настоящее согласие может быть мной отозвано при предоставлении в УЦ ВТБ (ПАО) заявления в простой письменной форме, содержащего номер основного документа, удостоверяющего мою личность, сведения о дате выдачи указанного документа и выдавшем его органе и мою собственноручную подпись.

«_____» _____ 20___ г. _____/_____/
подпись заявителя расшифровка подписи

_____
(заполняется уполномоченным работником Удостоверяющего центра Банк ВТБ (ПАО))

Данное Заявление о присоединении к Порядку зарегистрировано в реестре Удостоверяющего центра Банк ВТБ (ПАО).

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченный работник Удостоверяющего центра Банк ВТБ (ПАО)
_____/_____/
(подпись) (расшифровка подписи)

М.П.
«_____» _____ 20___ г.

Приложение 2 «Заявление на создание и выдачу квалифицированного сертификата»
к Порядку реализации функций аккредитованного удостоверяющего центра Банк ВТБ (ПАО) и исполнения его обязанностей

Форма заявления

В Удостоверяющий центр Банк ВТБ (ПАО)

ЗАЯВЛЕНИЕ
на создание и выдачу квалифицированного сертификата

Я,

_____,
(фамилия, имя, отчество)

_____
(серия и номер паспорта)

_____,
(кем и когда выдан)

Прошу:

☐ создать ключ электронной подписи
(поставить отметку либо зачеркнуть текст «создать ключ электронной подписи» при отказе от создания ключа удостоверяющим центром)

☒ создать квалифицированный сертификат ключа проверки электронной подписи (далее – Сертификат):

_____,
(Ф.И.О. полностью)

в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя: фамилия, имя, отчество	
Адрес электронной почты	
Город	
Область	
Страна	
СНИЛС	
ИНН налогоплательщика - физического лица	

Я,

_____,
(Ф.И.О владельца Сертификата – субъекта персональных данных)

даю согласие Банку ВТБ (ПАО) (ИНН 7702070139), адрес места нахождения: г. Санкт-Петербург, переулок Дегтярный, дом 11, литер А (далее – Оператор), на обработку моих персональных данных, а именно фамилии, имени и отчества, СНИЛС, пола, паспортных данных (серия и номер, код подразделения, место и дата рождения, дата и место выдачи паспорта, место регистрации) с правом осуществлять действия (операции) с персональными данными в целях создания и обслуживания Сертификата, формирования реестров выданных сертификатов, реестров аннулированных сертификатов, для регистрации, передачи в Единую систему идентификации и аутентификации и обслуживания в информационной системе Оператора, включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

- признаю, что персональные данные, заносимые в мой Сертификат, относятся к общедоступным персональным данным;
- ознакомлен и согласен с тем, что Оператор вправе хранить предоставленные копии документов и обрабатывать персональные данные посредством внесения их в электронную базу данных, списки (реестры) и отчетные формы;
- ознакомлен с условиями оказания услуг аккредитованным удостоверяющим центром Банка ВТБ (ПАО) и обязуюсь их выполнять. Согласен с Политикой Банка ВТБ (ПАО) в отношении обработки персональных данных и реализации требований к защите персональных данных и подтверждаю свое согласие на обработку персональных данных, в целях исполнения положений Федерального закона РФ №152-ФЗ от 27.07.2006г «О персональных данных».

Согласие на обработку персональных данных действует с момента подписания настоящего Заявления субъектом персональных данных бессрочно и может быть отозвано им в порядке, установленном Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Сведения в заявлении представлены на основании подлинных документов и являются достоверными.

Личная подпись владельца Сертификата (субъекта персональных данных**)** _____

«_____» _____ 20___ г.

Приложение 3 «Заявление о прекращении действия квалифицированного сертификата»
к Порядку реализации функций аккредитованного удостоверяющего центра Банк ВТБ (ПАО) и исполнения его обязанностей

Форма заявления

В Удостоверяющий центр Банка ВТБ (ПАО)

ЗАЯВЛЕНИЕ

о прекращении действия квалифицированного сертификата

Я, _____
(фамилия, имя, отчество)

паспорт серии _____ № _____ выдан _____
«____»

_____ _____ г., прошу аннулировать (отозвать) мой сертификат ключа проверки электронной подписи, в связи с

_____.
(причина отзыва сертификата)

Аннулируемый (отзываемый) сертификат содержит следующие данные:

Серийный номер сертификата ключа проверки электронной подписи	
Фамилия, имя, отчество	
СНИЛС	
ИНН налогоплательщика - физического лица	

_____/_____/
подпись заявителя расшифровка подписи

«_____» _____ 20___ г.

Приложение 4 «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи»
к Порядку реализации функций аккредитованного удостоверяющего центра Банк ВТБ (ПАО) и исполнения его обязанностей

РУКОВОДСТВО

ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ

ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ КВАЛИФИЦИРОВАННОЙ

ЭЛЕКТРОННОЙ ПОДПИСИ

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" и является средством информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

Применение электронной подписи может повлечь риск использования ключа электронной подписи третьими лицами вследствие несоблюдения мер защиты ключа электронной подписи от несанкционированного доступа.

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. N 152, в части обращения со средствами криптографической защиты информации;

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66, в части эксплуатации средств криптографической защиты информации;

- эксплуатационной документации к средствам электронной подписи;

- приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- личный пароль пользователь не имеет права никому сообщать;

- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;

- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;

- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

- необходимо предусмотреть меры, максимально ограничивающие доступ к:

- системному реестру;

- файлам и каталогам;

- временным файлам;

- журналам системы;

- файлам подкачки;

- кэшируемой информации (пароли и т.п.);

- отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

- организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

- регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.4. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.1.5. Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита;

- комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

- записывать на ключевые носители постороннюю информацию;

- оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации;

- использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;

- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

- должны регулярно устанавливаться обновления операционной системы;

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;

- должна быть активирована регистрация событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.