УТВЕРЖДЕН
Приказом Генерального директора ООО «ВБЦ»
от «22» марта 2018 № УЦ-03

Регламент
оказания услуг Удостоверяющего центра Общества с ограниченной ответственностью «ВБЦ»

Москва
2018

Оглавление

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Удостоверяющий центр - юридическое лицо, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г № 63-ФЗ «Об электронной подписи» (далее- Федеральный закон № 63-ФЗ).

Удостоверяющий центр Общества с ограниченной ответственностью «ВБЦ» (далее- Удостоверяющий центр, УЦ) осуществляет свою деятельность в качестве аккредитованного удостоверяющего центра на основании решения Минкомсвязи России регистрационный № 689 от 26 октября 2016 года, являющегося федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. С информацией по аккредитации Удостоверяющего центра Сторона, присоединившаяся к Регламенту оказания услуг удостоверяющего центра Общества с ограниченной ответственностью «ВБЦ» (далее- Регламент), может ознакомиться на официальном сайте Минкомсвязи России.

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании лицензии, выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России ЛСЗ № 0012785, регистрационный № 15226 Н от 21 июня 2016 года, соответствии с Постановлением Правительства Российской Федерации № 313 от 16 апреля 2012 года «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»**.**

Адрес: 123290, г. Москва, Мукомольный проезд 4а, стр. 2
ИНН 7703406864; **КПП** 770301001; **ОГРН** 1167746200489
Телефон/Факс: 8-495-215-57-43
E-mail: ca@vbankcenter.ru
Сайт: www.vbankcenter.ru
График работы: пн-пт с 09.00 до 19.00 (по Московскому времени)

2. ОПРЕДЕЛЕНИЯ И АКРОНИМЫ

2.1. Определения

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

Электронная подпись – 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.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

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

Заключением соглашения об использовании ПЭП является присоединение Заявителя к Регламенту ЭДО. Ключом ПЭП в Маркетплейсе ВБЦ могут являться:

- пара логин-пароль для входа в Личный кабинет в Маркетплейсе ВБЦ либо уникальный код-пароль, предоставленный Удостоверяющим центром Заявителю, после его идентификации. Введение Заявителем такого кода подтверждения позволяет Удостоверяющему центру определить лицо, поставившее ПЭП;
- сочетание номера подвижной (мобильной) связи, представленного Заявителем, и уникального случайно генерируемого кода аутентификации, отправленного Удостоверяющим центром на данный номер в форме SMS – сообщения;
- пароль ключа электронной подписи, позволяющий получить доступ к полному перечню государственных услуг, предоставляемых в электронном виде по имеющемуся идентификатору электронной подписи (Госуслуги – Единый портал государственных услуг и функций (ЕПГУ)).

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

Информация в электронной форме, подписанная ПЭП в Маркетплейсе ВБЦ, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Квалифицированная электронная подпись – усиленная электронная подпись, соответствующая следующим признакам:

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

- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром либо Доверенным лицом Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Владелец Сертификата – лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

При этом для Сертификата юридического лица вторым Владельцем является физическое лицо, данные о котором по заявлению юридического лица внесены в его Сертификат (Уполномоченный представитель Заявителя). В случаях, предусмотренных пунктом 3 статьи 14 Федерального закона № 63-ФЗ, данные о физическом лице в Сертификат не вносятся, единственным Владельцем сертификата является юридическое лицо. Для случаев выдачи Сертификата с указанием в Сертификате реквизитов только физического лица Владельцем сертификата является это физическое лицо.

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

Данные активации – закрытые данные, отличные от ключей, требуемые для управления ключевым носителем.

Идентификация – процесс, устанавливающий однозначное соответствие субъекта отличительным признакам.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Инфраструктура открытых ключей или (ИОК) – архитектура, организация, методики, способы и процедуры, которые обеспечивают управление и применение криптографической системы, основанной на сертификатах ключей проверки электронной подписи.

Компрометация ключа электронной подписи – результат действий физического лица, повлекший за собой разглашение ключа электронной подписи.

Список аннулированных (отозванных) сертификатов или СОС – электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список серийных номеров сертификатов, которые в определенный момент времени были отозваны, либо действие которых было приостановлено. Сертификаты, чьи номера присутствуют в списке файла СОС, являются отозванными из обращения Удостоверяющим центром.

Средства электронной подписи – 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.

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся работником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по созданию электронных подписей под выдаваемыми Удостоверяющим

центром Сертификатами в электронной форме и формируемыми Реестрами отозванных сертификатов, а также иными полномочиями согласно настоящему Регламенту.

Доверенное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по вручению ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром, а также иными полномочиями согласно настоящему Регламенту.

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

Сервисный центр – подразделение Удостоверяющего центра или действующее на основании договора с Удостоверяющим центром самостоятельное юридическое лицо/индивидуальный предприниматель, уполномоченные Удостоверяющим центром взаимодействовать с Заявителем.

Субъекты – это все лица, которые в силу настоящего Регламента, договора или действующего законодательства Российской Федерации обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Регламентом. Субъектами являются – Заявитель, Владелец Сертификата, Удостоверяющий центр.

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также физические лица.

Договор – Договор на оказание Услуг и поставку Продуктов Удостоверяющего центра.

Маркетплейс ВБЦ – программный и информационный сервис Общества с ограниченной ответственностью «ВБЦ» , имеющий адрес в сети Интернет vbankcenter.ru.

WEB-портал – выделенное место на интернет ресурсах vbankcenter.ru, epnow.ru, ucvbc.ru, ecpvbc.ru для публикации репозитория.

Регламент ЭДО – «Регламент взаимодействия и электронного документооборота в Маркетплейс ВБЦ» опубликованный в сети Интернет www.vbankcenter.ru.

44-ФЗ – Федеральный закон от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

223-ФЗ – Федеральный закон от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

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

152-ФЗ - Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2.2. Акронимы

ИОК Инфраструктура открытых ключей;
ПО Программное обеспечение;
ППС Политика применения сертификатов;
СОС Список аннулированных (отозванных) сертификатов;
СКЗИ Средства криптографической защиты информации;
УЦ Удостоверяющий центр;
ЦР Центр регистрации;
ЭП Электронная подпись;
КЭП Квалифицированная электронная подпись;
ПЭП Простая электронная подпись.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Назначение Регламента

Регламент, разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, и устанавливает общий порядок, условия предоставления и правила пользования услугами Удостоверяющего центра, в том числе права и обязанности, ответственность Владельца Сертификата, Заявителя и Удостоверяющего центра.

Регламент является договором присоединения на основании статьи 428 Гражданского кодекса Российской Федерации.

Лицо, присоединившееся к настоящему Регламенту обязано соблюдать его требования.

Регламент размещен для свободного доступа и ознакомления для всех заинтересованных лиц в электронной форме на сайте УЦ.

3.2. Изменение Регламента.

Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем размещения очередной редакции Регламента, включающей даты изменения (дополнения), на сайте Удостоверяющего центра.

3.3. Присоединение к Регламенту

Присоединение к Регламенту осуществляется путем предоставления заинтересованным лицом в Удостоверяющий центр Заявления на оказание услуг и поставку продуктов Удостоверяющего центра (создание сертификата ключа электронной подписи) или оплаты стоимости услуг и продуктов на основании выставленного счета Удостоверяющим центром в зависимости от того какое событие наступит раньше.

После присоединения к Регламенту Удостоверяющий центр и сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения.

С момента присоединения Заявителя к Регламенту, Заявитель полностью и безоговорочно соглашается со всеми условиями Регламента и приложений к нему.

Заявитель (Владелец Сертификата), присоединившийся к Регламенту, самостоятельно отслеживает изменения (дополнения), вносимые в Регламент в виде его новой редакции, путем самостоятельного ознакомления с текстом Регламента на сайте Удостоверяющего центра.

3.4. Перечень услуг Удостоверяющего центра

УЦ предоставляет следующие виды услуг:

- создание сертификатов ключей проверки электронной подписи в электронном виде и в форме документа на бумажном носителе;
- создание ключей ЭП и ключей проверки ЭП по обращениям Заявителей, с гарантией обеспечения конфиденциальности ключей ЭП;
- ведение Реестра выданных и аннулированных Сертификатов;
- аннулирование, приостановление и возобновление действия Сертификатов;

- предоставление копий Сертификатов в электронной форме, находящихся в Реестре изготовленных Сертификатов;
- предоставление сведений об аннулированных и приостановленных Сертификатах;
- проверка действительности ЭП, Ключи проверки которых содержатся в Сертификатах, выданных Удостоверяющим центром, в Электронных документах;
- распространение и техническое обслуживание средств ЭП;
- выдача Средств электронной подписи, обеспечивающих возможность создания Ключа электронной подписи и Ключа проверки;
- предоставление прав на использование программы для ЭВМ для управления сертификатом;
- предоставление услуг по сопровождению тарифного плана;
- предоставление иных связанных с использованием ЭП услуг.

3.5. Порядок оказания услуг

Оплата услуг по выпуску Сертификата осуществляется на основании выставленного счета авансовым платежом в размере 100 % (сто процентов) от стоимости оказываемых услуг. Заказчики, осуществляющие свою деятельность в рамках 44-ФЗ и 223-ФЗ, оплачивают услуги и продукты после подписания Сторонами Универсального передаточного документа (далее-УПД) в сумме, указанной в счете, выставленном Удостоверяющим центром.

Изготовление Сертификата происходит после осуществления следующих действий:

- представления Заявителем всех документов, необходимых для выпуска Сертификата;

- зачисление Заявителем денежных средств на расчетный счет УЦ (Центра выдачи или Сервисного центра) на основании выставленного счета Удостоверяющим центром (за исключением лиц, осуществляющих свою деятельность в рамках 44-ФЗ и 223-ФЗ).

3.6. Вознаграждение Удостоверяющего центра

Удостоверяющий центр осуществляет свою деятельность на платной основе. Стоимость и перечень услуг Удостоверяющего центра определяются тарифными планами, утвержденными Приказами УЦ ООО «ВБЦ», размещенными на сайте **www.vbankcenter.ru**, и проводимыми Удостоверяющим центром маркетинговыми акциями . Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим центром, регулируются условиями договоров Удостоверяющего центра.

Удостоверяющий центр в порядке, предусмотренном Регламентом, безвозмездно предоставляет Сертификаты в форме электронных документов из Реестра выданных Сертификатов Удостоверяющего центра, а также безвозмездно публикует Реестр отозванных Сертификатов.

3.7. Сроки действия Сертификатов

Максимальный срок использования ключа электронной подписи Удостоверяющего центра не более 3 (Трех) лет. Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи. Срок действия Сертификата Удостоверяющего центра не превышает 15 (Пятнадцати) лет.

Максимальный срок действия Ключа электронной подписи Заявителя устанавливается эксплуатационной документацией средства электронной подписи (системы криптографической защиты информации), с использованием которого такой Ключ создается.

Начало периода действия Ключа электронной подписи Заявителя исчисляется с момента начала действия Сертификата, соответствующего данному Ключу.

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

3.8. Использование Сертификата и ключа проверки электронной подписи Заявителем

Перед использованием Сертификата Заявитель обязан:

− в случае создания Сертификата в УЦ: ознакомиться под расписку с информацией, внесенной в Сертификат;

- в случае создания Сертификата на рабочем месте Заявителя: ознакомиться с информацией, внесенной в Сертификат и подтвердить с помощью КЭП;

− проверить статус используемого Сертификата и Сертификата УЦ.

Заявитель может использовать только действительный Сертификат.

3.9. Аннулирование (отзыв)

По истечении срока действия Сертификата он автоматически считается аннулированным. Сертификат считается аннулированным (отозванным), с момента публикации в репозитории УЦ списка аннулированных Сертификатов, содержащего информацию об изменении статуса этого Сертификата.

Удостоверяющий центр аннулирует Сертификат, если:

- не подтверждено, что Владелец Сертификата владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком Сертификате;
- установлено, что содержащийся в Сертификате Ключ проверки ЭП уже содержится в ином ранее созданном Сертификате;
- вступило в силу решение суда, которым установлено, что Сертификат содержит недостоверную информацию.

3.10. Кто имеет право подать запрос на отзыв

Запрос на отзыв Сертификата может быть подан:

− Владельцем Сертификата на основании заявления владельца Сертификата, подаваемого в форме документа на бумажном носителе, заверенного подписью и печатью (при наличии);

− уполномоченным представителем юридического лица (в случае изготовления Сертификата для сотрудника юридического лица) на основании заявления Владельца Сертификата, подаваемого в форме документа на бумажном носителе, заверенного подписью и печатью (при наличии);

− сотрудником УЦ, если он располагает достоверной информацией, требующей отзыва Сертификата.

3.11. Процедура рассмотрения запроса на аннулирование (отзыв) Сертификата

Запрос на аннулирование (отзыв) должен быть подан в Удостоверяющий центр (адрес: 123290, г. Москва, Мукомольный проезд 4а, стр. 2) на бумажном носителе и заверен подписью и печатью (при наличии).

Запрос должен содержать следующую информацию:

− серийный номер Сертификата или иную информацию, позволяющую однозначно идентифицировать Сертификат;

− причину аннулирования (отзыва) Сертификата;

− необходимые комментарии.

После получения запроса сотрудник УЦ производит верификацию запроса, и если таковая прошла успешно, то производит аннулирование (отзыв) Сертификата. После аннулирования (отзыва) Сертификата УЦ публикует обновленный СОС, содержащий информацию об аннулированном (отозванном) Сертификате.

Запрос на отзыв должен быть передан так быстро, насколько это возможно.

3.12. Срок, за который УЦ должен обработать запрос на аннулирование (отзыв)

Запрос на аннулирование (отзыв) рассматривается в течение 30 (тридцати) минут с момента его подачи. Временем подачи запроса считается:

− при вручении лично или передачей иными способами – время получения.

4. СТРУКТУРА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1. Центр сертификации

Центр сертификации (далее - ЦС) предназначен для: выпуска сертификатов Заявителям и сотрудникам УЦ, списков аннулированных (отозванных) Сертификатов (далее СОС), хранения эталонной базы Сертификатов и СОС.

ЦС взаимодействует только с ЦР или несколькими ЦР по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

ЦС самостоятельно не инициирует никаких соединений с ЦР, оставаясь пассивным слушателем. Инициирование соединения осуществляется ЦР по протоколу TLS с двухсторонней аутентификацией.

По протоколу HTTP допускается взаимодействие ЦР с ЦС только в рамках выполнения регламентных заданий по переносу СОС с ЦС на ЦР.

На ЦС находится эталонная база всех изготовленных Сертификатов.

К функциям ЦС относятся:

- генерация ключей и Сертификатов уполномоченного лица УЦ;
- смена ключей и Сертификатов уполномоченного лица УЦ;
- формирование Сертификатов по запросам ЦР;
- формирование запроса на кросс-сертификат уполномоченного лица УЦ;
- ведение базы данных Сертификатов с предоставлением доступа к ней ограниченному кругу компонентов системы;
- изменение базы данных Сертификатов по запросам от ЦР. Включает в себя аннулирование (отзыв) сертификатов;
- формирование СОС по запросам ЦР;
- формирование СОС в автоматическом режиме с периодичностью, заданной в расписании;
- ведение архива всех выпущенных СОС в автоматическом режиме;
- обеспечение уникальности следующей информации в Сертификатах:
  - ✓ ключ проверки электронной подписи;
  - ✓ серийный номер сертификата;
- взаимодействие с ЦР:
  - ✓аутентификация ЦР и определение прав доступа с использованием ключей и сертификатов ЦР;
  - ✓прием от ЦР запросов;
  - ✓проверка наличия подписи данной информации на ключе ЦР;
  - ✓обработка полученных от ЦР запросов; о передача на ЦР результатов обработки запросов;
  - ✓шифрование информации, передаваемой между ЦС и ЦР в ходе сетевого взаимодействия по протоколу TLS (КриптоПро TLS);
- протоколирование работы ЦС.

4.2. Центр регистрации

ЦР предназначен для хранения регистрационных данных владельцев Сертификатов, запросов на Сертификаты и Сертификатов.

ЦР взаимодействует с ЦС по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. По протоколу HTTP допускается взаимодействие ЦР с ЦС только в рамках выполнения регламентных заданий по переносу СОС с ЦС на ЦР.

ЦР является единственной точкой входа (регистрации) владельцев сертификатов в системе. Только зарегистрированные в ЦР субъекты (юридические или физические лица) могут получить Сертификат на свой ключ проверки электронной подписи в УЦ.

База данных ЦР (Реестр) содержит полную информацию и историю обо всех выпущенных Сертификатах для зарегистрированных на ЦР субъектов. К функциям ЦР относятся:

А) Обеспечение аутентификации приложений и сотрудников УЦ при обращении к ЦР;

Б) Ведение Базы Данных (Реестра), содержащей информацию о субъектах и их Сертификатах. База Данных содержит следующую информацию:

- данные о владельце Сертификата, включающиеся в сертификаты;
- данные о владельце Сертификата, не включаемые в сертификаты;
- ключи проверки электронной подписи владельцев, зарегистрированных в системе;
- Сертификаты, зарегистрированные в системе:
  - ✓действующие;
  - ✓отозванные (аннулированные, приостановленные);
  - ✓истекшим сроком действия Сертификата;
  - ✓с истекшим сроком действия ключа электронной подписи;

-запросы на регистрацию субъекта:

- ✓поступившие;
- ✓отвергнутые;
- ✓обработанные;

- запросы на выпуск Сертификатов:
  - ✓поступившие;
  - ✓отвергнутые;
  - ✓обработанные;
- запросы на отзыв Сертификатов:
  - ✓ поступившие;
  - ✓ отвергнутые;
  - ✓ Обработанные;

В) Управление политиками:

- политики уведомлений сотрудников УЦ и владельцев Сертификатов;
- политиками имен;
- политиками обработки запросов;
- политиками ролевой модели и системы разграничения доступа;

Г) Обеспечение уникальности следующей информации в Сертификатах:

- доменное имя владельца Сертификата;

Д) Взаимодействие с ЦС и внешними приложениям:

- прием от приложения и передача на ЦС запросов, подпись данных запросов на ключе ЦР;
- прием от ЦС и передача приложению результатов обработки запросов;
- проверка подписи ЦС на принимаемой от него информации;
- аутентификация и шифрование информации с использованием протокола TLS (КриптоПро TLS);

Е) Управление режимами работы УЦ по регистрации и управлению ключами и Сертификатами;

Ж) Обеспечение доступа к Базе Данных внешним приложениям через SOAP-интерфейс на базе HTTP(S);

З) Обеспечение выполнения ЦР в автоматическом режиме различных задач:

- ✓ оповещение владельцев Сертификатов и сотрудников УЦ по электронной почте о событиях, связанных с жизненным циклом Сертификатов (о регистрации субъекта, о изготовлении Сертификата, о отзыве Сертификата, об истечении срока действия Сертификатов, о необходимости замены ключей, и т.д.);
- ✓ получение СОС от соответствующего ЦС;
- ✓ получение СОС от ЦР вышестоящих по иерархии УЦ;
- ✓ удаление данных о зарегистрированных субъектах, не имеющих ни одного действующего Сертификата;
- ✓ протоколирование работы ЦР.

4.3. АРМ регистрации пользователя Центра Регистрации

АРМ регистрации пользователя ЦР предназначен для выполнения организационно технических мероприятий, связанных с выполнением процедуры регистрации субъекта в УЦ.
АРМ регистрации пользователя взаимодействует с ЦР по протоколу HTTP(S) с односторонней аутентификацией.
АРМ регистрации пользователя взаимодействует с АРМ формирования запроса на выпуск Сертификата по открытым каналам связи с применением СКЗИ для обеспечения целостности, конфиденциальности и аутентичности передаваемой информации.
К основным функциям АРМ регистрации пользователя ЦР относятся:

− обеспечение взаимодействия с ЦР;

− обеспечение взаимодействия с АРМ формирования запроса на выпуск Сертификата;

− обеспечение возможности проверки запроса на регистрацию субъекта в ЦР и передачи запроса на ЦР;

− обеспечение возможности проверки запроса на выпуск Сертификата и передача запроса на ЦР;

− регистрация субъектов в ЦР;

− организация просмотра информации из Базы Данных ЦР, относящейся к субъекту, зарегистрированному в системе;

− обеспечение возможности получения субъектом нескольких Сертификатов;

− проверка состояния и обработка запросов на формирование Сертификатов, поступающих от субъектов;

− шифрование информации, передаваемой между сотрудниками УЦ и ЦР, с использованием протокола TLS с односторонней аутентификацией.

4.4. АРМ формирования запроса на выпуск Сертификатов

АРМ формирования запроса на выпуск Сертификатов предназначен для выполнения организационно-технических мероприятий, связанных с выполнением процедуры проверки документов, предоставляемых Заявителем для формирования Сертификата и последующим созданием запроса на формирование Сертификата.
АРМ формирования запроса на выпуск Сертификатов взаимодействует с АРМ регистрации пользователя ЦР по открытым каналам связи с применением СКЗИ для обеспечения целостности, конфиденциальности и аутентичности передаваемой информации.

К основным функциям АРМ формирования запроса на выпуск Сертификатов относятся:

− генерация ключей;
− создание запросов на формирование Сертификатов;
− вывод Сертификата ключа проверки электронной подписи на бумажный носитель;
− создание запросов на приостановление/аннулирование (отзыв) Сертификатов;
− вывод Сертификата ЦС (уполномоченного лица УЦ) на бумажный носитель;
− сохранение СОС на отчуждаемом носителе в виде файла;
− сохранение Сертификата (цепочки Сертификатов) ЦС на отчуждаемом носителе в виде файла.

4.5. АРМ обработки запросов на аннулирование (отзыв) Сертификатов

АРМ формирования запроса на аннулирование (отзыв) Сертификатов предназначен для выполнения организационно-технических мероприятий, связанных с выполнением процедуры проверки документов, предоставляемых Пользователями УЦ для аннулирования (отзыва) Сертификата и последующим созданием запроса на отзыв Сертификата.

АРМ формирования запроса на аннулирование (отзыв) Сертификата взаимодействует с АРМ регистрации пользователя ЦР по защищённым каналам связи с применением СКЗИ для обеспечения целостности, конфиденциальности и аутентичности передаваемой информации.

К основным функциям АРМ формирования запроса на аннулирование (отзыв) Сертификатов относятся:

− удаление информации о зарегистрированных субъектах из ЦР, не имеющих ни одного действующего Сертификата;

− проверка состояния и обработка запросов на аннулирование (отзыв) Сертификатов, поступающих от Пользователей УЦ;

− просмотр протокола работы ЦР;

− публикация СОС.

5. ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИИ И ДОКУМЕНТОВ

5.1. Публикация

Удостоверяющий центр публикует на сайте в сети Интернет копии документов, на основании которых осуществляет свою деятельность.

5.2. Заверений копий

Заявитель для внесения сведений в Сертификат и для удостоверения личности Удостоверяющим центром предоставляет документы (сведения) или надлежащим образом заверенные копии документов, их подтверждающие.

Надлежащим способом заверения копий документов может являться:

- заверение копий документов Заявителем самостоятельно;
- нотариальное заверение копий;
- заверение копий органом власти (например, налоговыми органами);
- копии с документов могут быть сняты и заверены в том числе Доверенным лицом Удостоверяющего центра.

Копии, заверенные Заявителем, могут предоставлять исключительно юридические лица и индивидуальные предприниматели, имеющие собственную печать. Многостраничные копии либо должны быть прошиты и заверены на листе сшивки, либо на каждой странице такой копии должна иметься отдельная заверительная надпись. Образец заверительной надписи должен содержать: «копия верна», дату заверения документа, количество заверяемых листов, должность с указанием наименования организации/индивидуального предпринимателя, подпись, расшифровка подписи (фамилия и инициалы полностью), оттиск печати (для индивидуальных предпринимателей при наличии).

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

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

5.3. Предоставление сведений и документов для юридических лиц:

- основной документ, удостоверяющий личность Владельца Сертификата;
- основной документ, удостоверяющий личность получателя Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства);
- СНИЛС Владельца Сертификата;
- Доверенность, подтверждающая полномочия Владельца Сертификата ключа подписи (в случае, если Владелец Сертификата не имеет права действовать от имени юридического лица без доверенности). При использовании Маркетплейса ВБЦ полномочия Владельца Сертификата могут быть подтверждены цветной скан-копией доверенности, сделанной с оригинала, при условии полной оплаты, произведенной с расчетного счета Заявителя;
- Доверенность на получение сертификата ключа подписи (в случае, если Сертификат получает доверенное лицо, а не владелец Сертификата);
- Сведения об основном государственном регистрационном номере Заявителя или номер свидетельства о постановке на учет в налоговом органе Заявителя – иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или о идентификационном номере налогоплательщика Заявителя - иностранной

организации (указывается Заявителем в заявлении, которое направляется посредством электронной системы подачи заявлений УЦ, необходимом для выпуска сертификата).

5.4. Предоставление сведений и документов для индивидуальных предпринимателей:

- основной документ, удостоверяющий личность Владельца Сертификата;
- основной документ, удостоверяющий личность получателя Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства);
- СНИЛС Владельца Сертификата;
- Доверенность, подтверждающая полномочия Владельца Сертификата ключа подписи (в случае, если владелец Сертификата не имеет права действовать от лица Индивидуального предпринимателя без доверенности). При использовании Маркетплейса ВБЦ полномочия Владельца Сертификата могут быть подтверждены цветной скан-копией доверенности, сделанной с оригинала, заверенного подписью и печатью при условии полной оплаты, произведенной с расчетного счета Заявителя;
- Доверенность на получение сертификата ключа подписи (в случае, если Сертификат получает доверенное лицо, а не владелец Сертификата);
- Сведения об основном государственном регистрационном номере записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя (указывается Заявителем в заявлении, которое направляется посредством электронной системы подачи заявлений УЦ, необходимого для выпуска Сертификата).

5.5. Предоставление сведений и документов для физических лиц:

- основной документ, удостоверяющий личность Владельца Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства);
- СНИЛС Владельца сертификата;
- Идентификационный номер налогоплательщика;
- основной документ, удостоверяющий личность получателя Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства);
- Доверенность, нотариально заверенная, подтверждающая право действовать от имени Заявителя УЦ.

Основной документ, удостоверяющий личность, считается документом в рамках Федерального закона от 31 мая 2002 г. № 62-ФЗ «О гражданстве Российской Федерации» и Федерального закона от 25 июля 2002 г. № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации».

С примерами доверенностей можно ознакомиться сети Интернет по адресу **www.vbankcenter.ru**. Данные примеры носят исключительно ознакомительный характер. Актуальную форму Доверенности УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия.

Удостоверяющий центр вносит сведения в Сертификат при их полном совпадении с данными, указанными в едином государственном реестре юридических лиц (далее- ЕГРЮЛ) и едином государственном реестре индивидуальных предпринимателей (далее ЕГРИП).

Удостоверяющий центр выполняет свою обязанность по внесению в Сертификат только достоверной и актуальной информации путем сбора и хранения копий документов, представленных Заявителем.

Удостоверяющий центр оставляет за собой право запросить у стороны, присоединившейся к Регламенту, дополнительные документы, в случае предусмотренного законодательством установления операторами государственных, муниципальных информационных систем, а также иных информационных систем общего пользования, дополнительных требований к сертификатам ключа проверки электронной подписи пользователей соответствующих информационных систем для обеспечения информационной безопасности. Иные документы, подтверждающие сведения, включаемые в Сертификат Пользователя УЦ пунктом 8 части 2 статьи 17 Федерального закона № 63-ФЗ (в случае необходимости).

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

Документы и их надлежащим образом заверенные копии, представленные в Удостоверяющий центр для целей выдачи Сертификата, остаются на хранении в Удостоверяющем центре и возврату не подлежат.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1. Удостоверяющий центр обязан:

- предоставить Сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме Владельцу Сертификата;
- использовать для создания Ключа электронной подписи Удостоверяющего центра и формирования электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи;
- оказывать услуги в соответствии с требованиями, устанавливаемыми Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами в соответствии с законодательством Российской Федерации;
- использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им Сертификатов ключей проверки электронной подписи и списков, отозванных (аннулированных) Сертификатов;
- обеспечить защиту ключа электронной подписи Удостоверяющего центра от несанкционированного доступа;
- организовать свою работу по московскому времени и синхронизировать по времени все свои программные и технические средства обеспечения деятельности;
- обеспечить уникальность идентификационных данных Владельца Сертификата, заносимых в Сертификаты ключей проверки электронной подписи;
- создать Сертификат ключа проверки электронной подписи Владельца Сертификата по заявлению на создание Сертификата, в соответствии с порядком, определенным в Регламенте;
- обеспечить уникальность серийных номеров создаваемых Сертификатов.
- обеспечить уникальность значений ключей проверки электронной подписи в созданных Сертификатах УЦ;
- обеспечить сохранение в тайне созданного ключа электронной подписи пользователя Удостоверяющего центра;
- прекратить (аннулировать), приостановить и возобновить действие Сертификата Владельца Сертификата по соответствующему заявлению (Приложение№ 1, Приложение № 2 к Регламенту), в соответствии с порядком, определенным в Регламенте;
- прекратить действие Сертификата, если истек установленный срок, на который действие данного Сертификата было приостановлено;
- прекратить действие Сертификата в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра;
- официально уведомить об аннулировании, прекращении, приостановлении и возобновлении действия Сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации списка отозванных сертификатов;
- произвести регистрацию квалифицированного сертификата ЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ;
- публиковать актуальный список отозванных (аннулированных) Сертификатов на сайте Удостоверяющего центра;

- информировать в письменной форме Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;
- обеспечивать круглосуточную доступность Реестра отозванных сертификатов в сети Интернет, за исключением периодов планового или внепланового технического обслуживания;
- обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- 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;
- исполнять прочие обязанности, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и иными нормативными актами.

6.2. Заявитель обязан:

- предъявить документы, удостоверяющие личность Заявителя, доверенного лица Заявителя, Заявителя - физического лица в соответствии порядком предоставления информации Регламента;
- предоставить в Удостоверяющий центр документы, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем, и иные необходимые для создания Сертификата документы;
- по требованию Удостоверяющего центра обеспечить личную явку в Удостоверяющий центр определенных представителей Заявителя, а также совершить иные действия, направленные на обеспечение безопасности и законности процесса выдачи Сертификата (в том числе с использованием различных технических средств);
- совершать действия, направленные на обеспечение безопасности и законности процесса выдачи Сертификата (в том числе с использованием различных технических средств);
- уведомлять Удостоверяющий центр и иных участников электронного взаимодействия об изменении данных, указанных в заявлении на выдачу Сертификата со дня изменения таких данных.

6.3. Владелец Сертификата обязан:

- обеспечивать конфиденциальность Ключей электронных подписей;
- применять для формирования электронной подписи только действующий Ключ электронной подписи;
- применять Ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие ограничения были установлены.
- не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- немедленно обращаться в Удостоверяющий центр с заявлением на прекращение или приостановление действия Сертификата ключа проверки электронной подписи в случае

нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи (Приложение № 1 к Регламенту);

- не использовать ключ ЭП, связанный с Сертификатом ключа проверки электронной подписи, который аннулирован или действие которого приостановлено;
- при выдаче Сертификата ознакомиться с информацией, включаемой в Сертификат;
- предоставить заверенную копию Заявления на оказание услуг и поставку продуктов Удостоверяющего центра, Сертификат ключа проверки электронной подписи на бумажном носителе в формате электронного документа, подписанного с помощью электронной подписи в течение одного дня после получения сертификата электронной подписи;
- обеспечить выполнение правил по обеспечению безопасности на рабочем месте.

6.4. Участники электронного взаимодействия обязаны:

- обеспечивать конфиденциальность Ключей ЭП, в частности, не допускать использование принадлежащих им Ключей ЭП без их согласия;
- использовать ЭП в соответствии с ограничениями, содержащимися в Сертификате ключа проверки этой электронной подписи;
- уведомлять Удостоверяющий центр, выдавший Сертификат, и иных участников электронного взаимодействия о нарушении конфиденциальности Ключа электронной подписи со дня получения информации о таком нарушении;
- не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- использовать для создания и проверки ЭП, ключа проверки ЭП и ключа ЭП средства электронной подписи в соответствии с Федеральным законом № 63-ФЗ.

6.5. Права Удостоверяющего центра:

- запросить у Заявителя УЦ документы для подтверждения любой содержащейся в заявлении на выдачу Сертификата информации, а также документы, необходимые для разрешения противоречий между данными в заявлении на выдачу Сертификата и данными в иных представленных документах;
- Удостоверяющий центр вправе не принимать документы, не соответствующие требованиям действующих нормативных актов Российской Федерации и требованиям Регламента, а также в случае возникновения сомнений в подлинности предоставляемых документов;
- отказать в выдаче Сертификата в случае невыполнения обязанностей, установленных настоящим Регламентом, а также если услуга по созданию и выдаче Сертификата не оплачена в надлежащем порядке;
- отказать в создании Сертификата ключа проверки электронной подписи пользователю Удостоверяющего центра в случае не предоставления и/или предоставления не надлежаще оформленных документов (в неактуальной форме, с ошибками, исправлениями, подчистками и/или приписками), необходимых для Создания сертификата ключа проверки;
- отказать в аннулировании, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи в случае ненадлежащего оформления соответствующего заявления;
- отказать в аннулировании, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату;
- прекратить действие Сертификата в случае получения Удостоверяющим центром подтверждения факта смерти Владельца сертификата - физического лица, факта

внесения в Единый государственный реестр юридических лиц записи о ликвидации Владельца сертификата - юридического лица, факта утраты силы государственной регистрации Владельца сертификата - физического лица в качестве индивидуального предпринимателя;

- без уведомления приостановить и прекратить действие Сертификата в случае невыполнения Владельцем сертификата обязанностей, указанных в разделе 6.3 Регламента, а также в случае появления достоверных сведений о том, что документы, представленные в соответствии с разделом 6.2 настоящего Регламента, не являются подлинными или не подтверждают достоверность всей информации, включённой в данный Сертификат, и/или в случае, если услуга по созданию и выдаче данного Сертификата не оплачена в надлежащем порядке;
- отказать в прекращении действия Сертификата в случае ненадлежащего оформления Заявления на аннулирование (отзыв) Сертификата;
- отказать в выдаче Сертификата в случае, если не было подтверждено, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения Сертификата;
- в установленном порядке приостановить действие Сертификата, а также восстановить действие ранее приостановленного Сертификата.

6.6. Права Владельца Сертификата:

- обратиться в Удостоверяющий центр для прекращения действия выданного ему Сертификата в течение срока его действия;
- получить средства (средство) электронной подписи, получившие (получившее) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ, и неисключительную лицензию на право его использования (при выдаче программного или программно-аппаратного средства);
- получить от Удостоверяющего центра инструкции по обеспечению безопасности использования электронной подписи и Средств электронной подписи;
- получить Сертификат ключа проверки электронной подписи на бумажном носителе, заверенный Удостоверяющим центром;
- а также иные права, установленные законодательством Российской Федерации.

6.7. Права Участников электронного взаимодействия:

- использовать Реестр отозванных сертификатов для проверки действительности Сертификатов, созданных и выданных Удостоверяющим центром;
- получить Сертификат Удостоверяющего центра;
- получить Сертификат, находящийся в Реестре выданных сертификатов Удостоверяющего центра;
- применять Сертификат для проверки ЭП в электронных документах;
- обратиться в Удостоверяющий центр за проверкой подлинности ЭП, созданной с помощью Сертификата, выданного Удостоверяющим центром;
- при обращении за выдачей Сертификата получить информацию о рисках, связанных с использованием ЭП.

6.8. Ответственность субъектов

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

- если Удостоверяющий центр обоснованно полагался на сведения, представленные Заявителем;
- подделки, подлога либо иного искажения Заявителем, Владельцем сертификата либо третьими лицами информации, содержащейся в заявлении либо иных документах, представленных в Удостоверяющий центр.

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

Удостоверяющий центр не несет ответственность за упущенную выгоду.

Удостоверяющий центр не несет ответственность за ущерб, понесенный Владельцем сертификата в результате доверия к Сертификату, если Удостоверяющий центр выполнил все требования 63-ФЗ и Договора.

Удостоверяющий центр несет ответственность за сохранение конфиденциальной информации.

За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Удостоверяющий центр и Заявитель, Владелец Сертификата несут друг перед другом ответственность в размере и порядке, установленном действующим законодательством и заключенным Договором.

Владелец Сертификата несет ответственность за достаточность применяемых им мер по защите Ключа электронной подписи от компрометации, потери, уничтожения, изменения или иного неавторизованного использования.

Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации

7. СОЗДАНИЕ И ВЫДАЧА СЕРТИФИКАТА

Создание и выдача Сертификата осуществляется Удостоверяющим центром на основании Заявления на оказание услуг и поставку Продуктов Удостоверяющего центра. Заявление на оказание услуг и поставку Продуктов Удостоверяющего центра может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручно, в случае обращения Заявителя в Удостоверяющий центр, так и в электронном виде, подтвержденное ПЭП (введение кода-пароля), с учетом обязательной оплаты счета или КЭП Сертификат владельцу которой выдан любым аккредитованным удостоверяющим центром, Сертификат владельцу которой выдан Удостоверяющим центром ООО «ВБЦ».

С примерами заявлений на выдачу Сертификата можно ознакомиться сети Интернет по адресу **www.vbankcenter.ru**. Данные примеры носят исключительно ознакомительный характер. Актуальную форму Заявления на оказание услуг и поставку продуктов Удостоверяющего центра УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия.

Использование факсимиле (клише подписи) на Заявлении на оказание услуг и поставку продуктов Удостоверяющего центра не допускается.

Создание Ключей электронной подписи осуществляется Заявителем самостоятельно либо на своем рабочем месте, либо в Сервисном центре или Доверенным сотрудником УЦ (Центра выдачи).

Аутентификация Заявителя в Маркетплейсе ВБЦ производится с использованием логина и пароля или при помощи действующего Сертификата КЭП, созданного любым аккредитованным удостоверяющим центром.

Идентификация Заявителя в Маркетплейсе ВБЦ производится с введением Заявителем кода-пароля, полученного от Удостоверяющего центра (Центра выдачи) или Сервисного центра.

Удостоверяющим центром в Сертификат вносится информация на основании Заявления на оказание услуг и поставку продуктов Удостоверяющего центра. Если Владельцем Сертификата является юридическое лицо, то наряду с наименованием такого юридического лица в Сертификат может вноситься информация об Уполномоченном представителе. Удостоверяющий центр проверяет данные в Заявлении на оказание услуг и поставку продуктов Удостоверяющего центра на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

- факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно представляет;
- факт соответствия сведений, указанных в Заявлении на оказание услуг и поставку продуктов Удостоверяющего центра, представленным документам и, в необходимых случаях в соответствии с Федеральным законом № 63-ФЗ, информации, полученной из государственных реестров.

В случае внесения в Сертификат персональных данных физического лица, Заявитель – физическое лицо или Уполномоченный представитель Заявителя предоставляет свое согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в Заявление на оказание услуг и поставку продуктов Удостоверяющего центра.

Создание Сертификата производится в течение одного рабочего дня с момента формирования запроса на выпуск Сертификата.

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

По окончании процедуры создания Сертификата Владелец Сертификата получает:

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

Владелец Сертификата при получении Сертификата в Удостоверяющем центре подписывает собственноручно указанный Сертификат и тем самым подтверждает, что он ознакомлен Удостоверяющим центром с информацией, включенной в Сертификат. В отдельных случаях Удостоверяющий центр предоставляет возможность ознакомиться с информацией, включенной в Сертификат, в электронном виде, для подтверждения ознакомления с данной информацией Владелец Сертификата подписывает ее КЭП.

В момент выдачи (передачи) Сертификата или кода-пароля может осуществляться фото(видео)фиксация получателя Сертфиката или кода-пароля.

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

8. ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЭП В ЭЛЕКТРОННЫХ ДОКУМЕНТАХ

Подтверждение подлинности ЭП в электронном документе, авторство или содержание которого оспаривается, осуществляется на основании заявления на подтверждение подлинности ЭП, форма которого размещена на сайте Удостоверяющего центра.

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

Срок проведения работ по подтверждению подлинности ЭП в электронном документе составляет до 10 (десяти) рабочих дней с момента поступления заявления в Удостоверяющий центр и при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

9. КОНФИДЕНЦИАЛЬНОСТЬ

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

Удостоверяющий центр обеспечивает конфиденциальность персональных данных, вносимых в Реестр сертификатов.

10. ХРАНЕНИЕ ИНФОРМАЦИИ

Архивированию подлежат следующая документированная информация:

- реестр сертификатов ключей проверки электронной подписи Владельцев Сертификата Удостоверяющего центра;
- сертификаты ключей проверки электронной подписи уполномоченного лица Удостоверяющего центра;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- заявления на прекращение действия сертификата ключа проверки электронной подписи;
- заявления на приостановку/аннулирование (отзыв) действия сертификата ключа проверки электронной подписи (Форма –Приложение № 1 к Регламенту);
- заявления о возобновлении действия сертификата ключа проверки электронной подписи (Форма – Приложение № 2 к Регламенту);
- внутренние документы Удостоверяющего центра.

Архив документации Удостоверяющего центра подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Удостоверяющего центра и назначаемой приказом руководителя Удостоверяющего центра.

11. РЕПОЗИТОРИЙ И ПУБЛИКАЦИЯ ИНФОРМАЦИИ

УЦ поддерживает в актуальном состоянии репозиторий. В качестве репозитория используется выделенная директория на WEB-портале.

Публикации подлежит:

− сертификат Центра сертификации УЦ;
− список аннулированных сертификатов;
− регламент применения сертификатов (настоящий Регламент УЦ);
− шаблоны заявлений на выпуск сертификата;
− сведения об аттестации и аккредитации;
− сопутствующая информация, уведомления, обновления и исправления.

Публикация информации осуществляется, как только она становится доступной и с частотой необходимой для поддержания ее в актуальном состоянии.

Вся публикуемая информация является общедоступной для Субъектов УЦ. Администратор репозитория использует различные механизмы для предотвращения неавторизованного изменения, дополнения и/или удаления опубликованной информации.

12. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Генерация и инсталляция ключевых пар

Генерация ключевых пар

Генерация ключевых пар может производиться Заявителем самостоятельно или сотрудником УЦ. Генерация ключевых пар осуществляется на ключевые носители, требования к которым приведены в разделе Регламента «Стандарты и контроль криптографических модулей».

Передача ключа электронной подписи

В случае, если генерация ключевой пары осуществляется сотрудником УЦ, то передача ключа электронной подписи осуществляется путем передачи ключевого носителя. Ключевой носитель передается способом, гарантирующим конфиденциальность ключа электронной подписи.

Передача ключа проверки электронной подписи издателю сертификата

При создании запроса на Сертификат Заявителем, он может передать ключ проверки электронной подписи в УЦ в составе подписанного запроса формата PKCS#10, при этом запрос подписывается с применением ключа электронной подписи, соответствующего действующему сертификату.

При создании запроса на сертификат оператором УЦ дополнительных требований к передаче ключа проверки электронной подписи не предъявляется.

Передача ключа проверки электронной подписи центра сертификации пользователям УЦ

Ключ проверки электронной подписи ЦС содержится в его Сертификате. Сертификат ЦС опубликован в репозитории на WEB-портале по URL-адресам: http://ucvbc.ru/vbc01.crt, http://ecpvbc.ru/crl/vbc01.crt.

Размеры ключей

Длина ключей электронной подписи следующая:

− ключ электронной подписи - 256 бит;

− ключ проверки электронной подписи - 512 бит (на базе ГОСТ Р 34.10-2001).

Длина ключей электронной подписи, используемых для шифрования должна быть следующей:

− сессионный ключ для шифрования (по ГОСТ 28147-89) - 256 бит;

− ключ электронной подписи - 256 бит;

− ключ проверки электронной подписи - 512 бит (на базе ГОСТ Р 34.10-2001).

Генерация параметров ключа проверки электронной подписи и проверка качества

В соответствии с действующей политикой и системой менеджмента качества.

Защита ключа электронной подписи и технический контроль криптографических модулей

Стандарты и контроль криптографических модулей

Формирование ключей электронной подписи производится на следующие типы носителей:

− процессорные карты MPCOS-EMV, российские интеллектуальные карты (РИК), интеллектуальные карты "Оскар" с использованием считывателей смарт-карт, поддерживающий протокол PS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126);

− таблетки Touch-Memory DS1993 – DS1996 с использованием устройств Аккорд 4+, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS;

− сертифицированные электронные носители с интерфейсом USB;

− съемные носители с интерфейсом USB (только в случае генерация ключевой пары Клиентом);

− реестр ОС Windows (только в случае генерация ключевой пары Клиентом).

Резервная копия ключа электронной подписи

Резервное копирование и хранение резервных копий ключей электронной подписи компонентов УЦ осуществляется с использованием методов и средств, обеспечивающих уровень защищенности не меньше уровня защищенности ключевого носителя.

Перенос ключа электронной подписи из/в криптографический модуль

Перенос ключа электронной подписи из криптографического модуля или в криптографический модуль осуществляется методами, гарантирующими его нераспространение.

Хранение ключа электронной подписи в криптографическом модуле

Ключ электронной подписи хранится в криптографическом модуле в зашифрованном виде.

Метод активации ключа электронной подписи

Активация ключа электронной подписи может осуществляться только его владельцем. Для активации ключа электронной подписи должны использоваться данные активации, удовлетворяющие требованиям раздела «Данные активации». Активация ключа электронной подписи должна производиться на ограниченный период времени.

Метод деактивации ключа электронной подписи

Деактивация ключа электронной подписи должна производиться либо автоматически, либо путем отключения ключевого носителя.

Метод уничтожения ключа электронной подписи

После окончания срока действия или архивного хранения, если таковое осуществляется, ключ электронной подписи уничтожается методами, гарантирующими невозможность его восстановления.

Данные активации

Генерация и инсталляция данных активации

Данные активации используются для защиты ключевых носителей. Данные активации создаются перед генерацией ключевой пары. УЦ может не осуществлять создание данных активации для клиентов.

В качестве данных активации могут быть использованы:

− пароль, PIN;

− биометрическая информация;

− системы строгой двухфакторной аутентификации.

Для всех политик применения сертификатов пароль (PIN) должен отвечать следующим требованиям:

− известен только владельцу;

− длина не менее 8 символов;

− мощность алфавита не менее 10 символов;

− не должен содержать слов, словосочетаний, имен и т.п.

Защита данных активации

Данные активации должны защищаться от потери, порчи, неавторизованного использования или раскрытия.

Другие аспекты, относящиеся к данным активации

Передача или уничтожение данных активации должны осуществляться методами, обеспечивающими невозможность потери, кражи, разглашения, порчи, модификации или неавторизованного использования.

Средства управления безопасностью вычислительной техники

Особые технические требования по безопасности вычислительной техники

Используемая вычислительная техника обеспечивает сохранность и защиту данных УЦ и ключей электронной подписи от уничтожения, порчи, модификации, разглашения или неавторизованного использования.

Оценка безопасности вычислительной техники

Программное обеспечение и аппаратные средства защиты, осуществляющие работу с ключевой информацией, сертифицированы ФСБ РФ.

Технические средства управления жизненным циклом

Средства управления организацией безопасности

УЦ использует механизмы проверки безопасной конфигурации и целостности используемых систем.

Средства управления сетевой безопасностью

УЦ использует средства сетевой безопасности, предотвращающие неавторизованный доступ к информации и защищающие от атак.

13. ПЕРСОНАЛЬНЫЙ ДАННЫЕ

13.1. Обработка персональных Владельца сертификата Удостоверяющего центра:

13.1.1. Цель обработки: идентификация и аутентификация субъекта персональных данных в качестве по Владельца сертификата, а также пользователя информационных систем с применением ЭП, в которых используются сертификаты ключей подписи Владельца сертификата.

13.1.2. Персональные данные, обрабатываемые УЦ: фамилия, имя, отчество, паспортные данные, СНИЛС, идентификационный номер налогоплательщика. В Сертификат, изготавливаемый УЦ, вносят фамилию, имя, отчество, СНИЛС, идентификационный номер налогоплательщика.

13.1.3. Персональные данные, вносимые в СКПЭП относятся к категории общедоступных.

13.1.4. УЦ осуществляет действия по сбору, записи, систематизации, накоплению, использованию, хранению, уточнению, обновлению, изменению, блокированию и уничтожению персональных данных Владельцев сертификатов в соответствии с 152-ФЗ.

13.1.5. УЦ не раскрывает третьим лицам и не распространяет персональные данные Владельца сертификата без письменного его согласия на раскрытие данной информации, за исключением случаев, прямо установленных законодательством Российской Федерации.

13.1.6. Согласие на обработку персональных данных может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Владельца сертификата при удовлетворении которого, впоследствии УЦ отзываются все выпущенные сертификаты Владельца сертификата.

14. СТРУКТУРА СЕРТИФИКАТОВ

14.1 Структура квалифицированного сертификата

Структура квалифицированного сертификата должна соответствовать требованиям Приказа ФСБ от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Все издаваемые квалифицированные сертификаты содержат следующие базовые поля:

Serial Number - уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов УЦ;

Signature Algorithm - объектный идентификатор алгоритма, используемого для подписи сертификата;

Issuer - отличительное имя ЦС или идентификационные данные Уполномоченного лица УЦ;

Valid From - дата начала действия сертификата;

Valid To - дата окончания действия сертификата;

Subject - идентификационные данные владельца сертификата;

Subject Public Key - ключ проверки электронной подписи владельца сертификата;

Version - версия структуры сертификата формата X.509;

Signature - ЭП Уполномоченного лица УЦ.

14.2 Расширения квалифицированного сертификата

В издаваемых квалифицированных сертификатах могут использоваться только перечисленные в данном разделе расширения. В случае, если значение какого-либо поля (флага) перечисленных расширений не определено данным документом, УЦ вправе определить значение данного поля для издаваемых квалифицированных сертификатов в соответствии с требованиями X.509 и RFC 5280.

- Authority Key Identifier

Данное расширение обязательно для всех сертификатов, за исключением самоподписанных сертификатов ЦС, и является некритическим. Это расширение должно обязательно содержать поле keyIdentifier, в котором содержится идентификатор ключа проверки электронной подписи издателя. Остальные поля не обязательны.

- Subject Key Identifier

Данное расширение обязательно для всех сертификатов, является некритическим и содержит идентификатор ключа проверки электронной подписи владельца сертификата.

- KeyUsage

Данное расширение обязательно для всех сертификатов и является критическим.
Значения полей расширения KeyUsage:

Поле	**Сертификат ЦС**	**Сертификаты клиентов**
digitalSignature	0	0/1
nonRepudiation	0	0/1
keyEncipherment	0	0/1
dataEncipherment	0	0/1
keyAgreement	0	0/1
keyCertSign	1	0
CRLSign	1	0
encipherOnly	0	0/1
decipherOnly	0	0/1

- Certificate Policies

Данное расширение должно присутствовать во всех сертификатах клиентов, содержать объектные идентификаторы ППС, в соответствии с которыми он выдан. Для сертификата Центра сертификации рекомендуется использование данного расширения, но в случае отсутствия такового в сертификате ЦС считается, что такой сертификат выпущен для любой политики. Расширение является некритическим.

- Policy Mappings

Данное расширение может использоваться только в кросс-сертификатах и быть некритическим.

- Basic Constraints

Расширение должно содержаться в сертификате ЦС и является критическим. Значение флага CA установлено в 1 (true). Расширение сертификата ЦС так же содержит поле pathLenConstraint, значение которого установлено в 0 (ноль).

- CRL Distribution Points

Данное расширение должно содержаться во всех сертификатах клиентов, быть некритическим и содержать последовательность точек доступа к списку аннулированных сертификатов ЦС.

- Inhibit Any-Policy

Данное расширение может содержаться только в кросс-сертификатах, и в случае использования должно быть критическим.

- Authority Information Access

Расширение должно присутствовать во всех сертификатах Клиентов, быть некритическим и содержать URL-адреса точек публикации сертификата Центра сертификации и URL-адреса OCSP и TSP служб.

- Extended Key Usage

Данное расширение присутствует в сертификатах клиентов и является некритическим. Расширение содержит объектные идентификаторы областей использования сертификатов, предусмотренных ППС, в соответствие с которыми выпущен сертификат.

Объектные идентификаторы криптографических алгоритмов

Все участники ИОК должны использовать в своей работе криптографические алгоритмы с объектными идентификаторами, соответствующими RFC 3279, RFC 4491.

Формы имен

В квалифицированном сертификате поля идентификационных данных Уполномоченного лица Удостоверяющего центра и Владельца сертификата содержат атрибуты имени формата X.500.

Ограничения имен

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

Common Name: Наименование ПАК УЦ, для которого выпущен данный сертификат;

Organization: Наименование организации, являющейся владельцем Удостоверяющего центра;

Organization Unit: Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего центра;

Email: Адрес электронной почты;

Country: Буквенный код страны (например, RU);

State: Субъект Федерации, где зарегистрирована организация, являющейся владельцем Удостоверяющего центра;

STREET: Адрес регистрации организации, являющейся владельцем Удостоверяющего центра;

INN: ИНН организации, являющейся владельцем Удостоверяющего центра;

OGRN: ОГРН организации, являющейся владельцем Удостоверяющего центра;

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего собственные интересы, являются:

Common Name: Фамилия, имя, отчество;
surname: Фамилия Владельца сертификата;
givenName: Имя и отчество Владельца сертификата;
Organization: Только для ИП – наименование согласно выписке из ЕГРИП;
Email: Адрес электронной почты;
Country: буквенный код страны (например, RU);
STREET: Адрес регистрации Владельца сертификата;
INN: ИНН Владельца сертификата;
OGRNIP: Только для ИП - ОГРНИП;
SNILS: СНИЛС Владельца сертификата;

Обязательными атрибутами поля идентификационных данных Владельца сертификата, представляющего интересы юридического лица, являются:

Common Name: Наименование организации, которую представляет Владелец сертификата;
surname: Фамилия Владельца сертификата;
givenName: Имя и отчество Владельца сертификата;
Organization: Наименование организации, которую представляет Владелец сертификата;
Organization Unit: Наименование подразделения организации, сотрудником которого является Владелец сертификата;
Email: Адрес электронной почты;
Country: буквенный код страны (например, RU);
State: Субъект Федерации, где зарегистрирована организация, которую представляет Владелец сертификата;
STREET: Адрес регистрации юр. лица;
INN: ИНН юр. лица с двумя ведущими нолями;
OGRN: ОГРН юр. лица;
SNILS: СНИЛС Владельца сертификата;

14.3 Структура неквалифицированного сертификата, формируемого Авторизованным удостоверяющим центром для участника электронных аукционов

Неквалифицированный сертификат ключа проверки электронной подписи, издаваемый Удостоверяющим центром для участника электронных аукционов, должен соответствовать стандарту X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Все издаваемые неквалифицированные сертификаты содержат следующие базовые поля:

− **Serial Number** - уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов УЦ;

− **Signature Algorithm** - объектный идентификатор алгоритма, используемого для подписи сертификата;

− **Issuer** - отличительное имя ЦС или идентификационные данные Уполномоченного лица УЦ;

− **Valid From** - дата начала действия сертификата;

− **Valid To** - дата окончания действия сертификата;

− **Subject** - идентификационные данные владельца сертификата;

− **Subject Public Key** - ключ проверки электронной подписи владельца сертификата;

− **Version** - версия структуры сертификата формата X.509;

− **Signature** - ЭП Уполномоченного лица УЦ.

Номер версии

Версия издаваемых сертификатов не ниже 3.

Расширения сертификата

В издаваемых неквалифицированных сертификатах могут использоваться только перечисленные в данном разделе расширения. В случае если значение какого-либо поля (флага) перечисленных расширений не определено данным документом, УЦ вправе определить значение данного поля для издаваемых неквалифицированных сертификатов в соответствии с требованиями X.509 и RFC 5280.

- Authority Key Identifier

Данное расширение обязательно для всех сертификатов и является некритическим. Это расширение должно обязательно содержать поле keyIdentifier, в котором содержится идентификатор ключа проверки электронной подписи издателя. Остальные поля не обязательны.

- Subject Key Identifier

Данное расширение должно присутствовать во всех сертификатах, являться некритическим и содержит идентификатор ключа проверки электронной подписи владельца сертификата.

- KeyUsage

Данное расширение должно присутствовать во всех сертификатах и быть критическим. Значения полей расширения KeyUsage:

Поле	**Сертификат ЦС**	**Сертификаты клиентов**
digitalSignature	0	0/1
nonRepudiation	0	0/1
keyEncipherment	0	0/1
dataEncipherment	0	0/1
keyAgreement	0	0/1
keyCertSign	1	0

CRLSign	1	0
encipherOnly	0	0/1
decipherOnly	0	0/1

- Certificate Policies

Данное расширение должно присутствовать во всех сертификатах, содержать объектные идентификаторы ППС, в соответствии с которыми он выдан. Расширение является некритическим.

- Policy Mappings

Данное расширение может использоваться только в кросс-сертификатах и быть некритическим.

- Basic Constraints

Расширение должно содержаться в сертификате ЦС и является критическим. Значение флага CA установлено в 1 (true). Расширение сертификата ЦС так же содержит поле pathLenConstraint, значение которого установлено в 0 (ноль).

- CRL Distribution Points

Данное расширение должно содержаться во всех сертификатах клиентов, быть некритическим и содержать последовательность точек доступа к списку аннулированных сертификатов ЦС.

- Inhibit Any-Policy

Данное расширение может содержаться только в кросс-сертификатах, и в случае использования должно быть критическим.

- Authority Information Access

Расширение должно присутствовать во всех сертификатах Клиентов, быть некритическим и содержать URL-адреса точек публикации сертификата Центра сертификации и URL-адреса OCSP и TSP служб.

- Extended Key Usage

Данное расширение присутствует в сертификатах и является некритическим. Расширение содержит объектные идентификаторы областей использования сертификатов, предусмотренных ППС, в соответствие с которыми выпущен сертификат.

Объектные идентификаторы криптографических алгоритмов

Все участники ИОК должны использовать в своей работе криптографические алгоритмы с объектными идентификаторами, соответствующими RFC 3279, RFC 4491.

Формы имен

В неквалифицированном сертификате поля идентификационных данных Уполномоченного лица Удостоверяющего центра и Владельца сертификата содержат атрибуты имени формата X.500.

Ограничения имен

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего собственные интересы, являются:

Common Name: Фамилия, имя, отчество владельца сертификата;

surname: Фамилия владельца сертификата;

givenName: Имя и отчество владельца сертификата;

Email: Адрес электронной почты;

Country: буквенный код страны (например, RU);

STREET: Адрес регистрации физ. лица;

INN: ИНН физ. лица;

OGRNIP: Только для ИП - ОГРНИП;

UnsructuredName: INN=ИНН физ. лица;

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего интересы юридического лица, являются:

Common Name: Фамилия, имя, отчество владельца сертификата;

surname: Фамилия владельца сертификата;

givenName: Имя и отчество владельца сертификата;

Organization: Наименование организации, которую представляет владелец сертификата;

Organization Unit: Наименование подразделения организации, сотрудником которого является владелец сертификата;

Email: Адрес электронной почты;

Country: буквенный код страны (например, RU);

State: Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата;

STREET: Адрес регистрации юр. лица;

INN: ИНН юр. лица с двумя ведущими нолями;

OGRN: ОГРН юр. лица;

SNILS: СНИЛС владельца сертификата;

UnsructuredName: INN=ИНН юр. лица/KPP=КПП юр. лица /OGRN=ОГРН юр. лица;

14.4 Структура списков аннулированных сертификатов

Структура списков аннулированных сертификатов должна соответствовать RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Списки аннулированных сертификатов содержат следующие основные поля:

− **Version** – версия структуры COC формата X.509;

− **Signature Algorithm** - объектный идентификатор алгоритма, используемого для подписи CRL;

− **Signature** - ЭП Уполномоченного лица УЦ.

− **Issuer** - отличительное имя ЦС или идентификационные данные Уполномоченного лица УЦ;

− **This Update** - дата и время выпуска текущего CRL;

− **Next Update** - дата и время планового выпуска следующего CRL;

− **Next Publication** - дата и время следующей плановой публикации CRL;

− **Revoked Certificates** - список аннулированных (отозванных) сертификатов, включающий серийный номер сертификата и дату отзыва. Данное поле может отсутствовать, если нет отозванных сертификатов.

Номер версии

Все издаваемые СОС версии 2.

Расширения CRL и элементов CRL

- **Authority Key Identifier**

Идентификатор ключа Центра сертификации, которым подписан данный СОС.

- **CRL Number**

Некритическое рекомендуемое расширение, содержащее порядковый номер СОС.

- **Reason Code**

Некритическое рекомендуемое расширение элемента CRL, содержащее причину отзыва сертификата.

Приложение № 1
к Регламенту оказания услуг удостоверяющего центра
Общества с ограниченной ответственностью «ВБЦ»

ФОРМА

Заявление
на приостановку/аннулирование (отзыв)
сертификата ключа проверки электронной подписи

_____
(фамилия, имя, отчество)

_____
(Для ЮЛ: должность, название организации)

Просит

□ приостановить на _____дней

□ аннулировать (отозвать)

сертификаты ключей проверки электронной подписи:

№	ФИО	Должность (для ЮЛ)	Серийный номер сертификата
1.			

По причине:

_____
(причина отзыва сертификата)

_____ _____
(подпись) (фамилия, инициалы)

«____»_____ 201__ г. М.П

Приложение № 2
к Регламенту оказания услуг удостоверяющего центра
Общества с ограниченной ответственностью «ВБЦ»

ФОРМА

Заявление
о возобновлении действия сертификата ключа электронной подписи

_____
(фамилия, имя, отчество)

_____
(Для ЮЛ: должность, название организации)

Просит возобновить действие приостановленных сертификатов ключей электронной подписи:

№	ФИО	Должность (для ЮЛ)	Серийный номер сертификата
1.			

_____ _____
(подпись) (фамилия, инициалы)

«____»_____ 201__ г. М.П

Приложение № 3
к Регламенту оказания услуг удостоверяющего центра
Общества с ограниченной ответственностью «ВБЦ»

Руководство по обеспечению безопасности использования средств криптографической защиты информации

Владелец Сертификата обязан:
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств квалифицированной электронной подписи;
- сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи средств квалифицированной электронной подписи, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;
- обеспечивать конфиденциальность ключей электронной подписи, в частности не допускать использование принадлежащих ему ключей электронной подписи без его согласия;
- уведомлять Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированной электронной подписи и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с действующим Федеральным законодательством;
- не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр для прекращения действия сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены);
- обновлять сертификат ключа проверки электронной подписи в соответствии с установленным Регламентом;
- принять меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средством квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, технические средства, на которых эксплуатируется средства квалифицированной электронной подписи и защищаемую информацию.

Владельцу Сертификата запрещается:
- оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- использовать нестандартные, изменённые или отладочные версии операционных систем;
- подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором;
- обрабатывать на ПЭВМ, оснащённой средством квалифицированной электронной подписи, информацию, содержащую государственную тайну.

Владелец несёт ответственность за:
- полноту и своевременность предоставления документов в УЦ;
- обеспечение конфиденциальности ключей электронной подписи, в частности не допущение использования принадлежащих ему ключей электронной подписи без его согласия;
- уведомление Удостоверяющего центра, выдавшего сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использование ключа электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.