Приложение № 1

УТВЕРЖДЕН
Приказом Генерального директора ООО «ВБЦ»
от «19» сентября 2017 № УЦ-04

Регламент
удостоверяющего центра
Общества с ограниченной ответственностью
«ВБЦ»

Москва
2017

Оглавление

Сведения об Удостоверяющем центре

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 Удостоверяющего центра (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)».

Юридический адрес: 123290, г. Москва, Мукомольный проезд 4а, стр. 2
Почтовый адрес: 123290, г. Москва, Мукомольный проезд 4а, стр. 2
ИНН 7703406864; **КПП** 770301001; **ОГРН** 1167746200489
Телефон/Факс: 8-495-215-57-43
Email: ca@vbankcenter.ru
Сайт: **www.vbankcenter.ru**
График работы: пн-пт с 09.00 до 21.00

Определения и акронимы

Определения

Аутентификация — процесс, устанавливающий, что субъект является тем за кого себя выдает.

Владелец сертификата – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат, владеющее ключом электронной подписи, соответствующим ключу проверки электронной подписи, включенному в состав сертификата, выданного на его имя.

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

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

Заявитель УЦ — субъект, подавший заявление на выпуск сертификата.

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.

Квалификатор политики — зависимая от Политики применения сертификатов (ППС) информация, которая может сопутствовать идентификатору ППС в сертификате X.509.

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

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

Пользователь УЦ— субъект, применяющий выпущенный согласно настоящему Регламенту УЦ сертификат, и который действует, доверяя этому сертификату и/или любой ЭП проверенной с использованием этого сертификата.

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.

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 заверению сертификатов и СОС.

Электронный документ - форма подготовки, отправления, получения или хранения информации с помощью электронных технических средств, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе.

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.

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.

Общие положения

Назначение Регламента

Регламент, разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, и устанавливает общий порядок и условия предоставления удостоверяющим центром услуг по изготовлению сертификатов ключей подписи и дополнительных услуг, связанных с управлением сертификатами ключей подписи.

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

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

Изменение Регламента.

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

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

Присоединение к Регламенту

Фактом о присоединении к Регламенту Заявителем УЦ является регистрация им на сайте Личного кабинета и наиболее раннее из наступивших событий: подача заявления и отправки документов Заявителем УЦ посредством электронной системы подачи заявлений УЦ, необходимых для выпуска сертификата или момент предоставления Заявителем УЦ документов, необходимых для выпуска сертификата.

Получение Удостоверяющим центром документов, необходимых для изготовления сертификата, считается присоединением Заявителя УЦ к Регламенту, и он будет являться Стороной Регламента.

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

Пользователь УЦ, 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.

Перечень услуг

УЦ предоставляет пользователям УЦ следующие виды услуг:

- изготовление сертификатов ключей проверки электронной подписи (далее-Сертификат) 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;
- подтверждение подлинности ЭП в документах, представленных в электронной форме;
- подтверждение подлинности ЭП Удостоверяющего центра в изготовленных им Сертификатах;
- распространение и техническое обслуживание средств ЭП;
- предоставление иных связанных с использованием ЭП услуг.

Порядок оказания услуг

Оплата услуг по выпуску Сертификата осуществляется на основании выставленного счета авансовым платежом в размере 100 % (сто процентов) от стоимости оказываемых услуг.

Изготовление Сертификата происходит после осуществления следующих действий в совокупности:

- представления Заявителем УЦ всех документов, необходимых для выпуска Сертификата;
- зачисление перечисленных Заявителем УЦ денежных средств на расчетный счет УЦ.

В случае соблюдения указанных требований, в соответствии с п. 3 ст. 434 и п. 3 ст. 438 ГК РФ, оплаченные денежные средства не возвращаются.

Разъяснения касательно деятельности и порядка оказания услуг Удостоверяющим центром может получить любое лицо при подаче соответствующего запроса, оформленного в надлежащем письменном виде и заверенное уполномоченным лицом направленное на юридический адрес УЦ.

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». Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим центром, регулируются условиями договоров между Удостоверяющим центром и Заявителем УЦ. 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.

Сроки действия Сертификатов

Срок действия ключа электронной подписи пользователя Удостоверяющего центра составляет 1 (Один) год. Начало периода действия ключа электронной подписи пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи. Срок действия Сертификата не превышает 12 (двенадцать) месяцев

Использование Сертификата и ключа проверки электронной подписи Заявителем УЦ

Перед использованием Сертификата Заявитель УЦ обязан:

− ознакомиться с политиками применения Сертификатов и Регламентом УЦ, в соответствии с которыми выдан Сертификат;

− проверить статус используемого Сертификата и Сертификата УЦ.

Заявитель УЦ может использовать только действительный Сертификат, в соответствии с требованиями его политики.

Аннулирование

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.

Обстоятельства отзыва Сертификата

Сертификат может быть отозван/аннулирован при следующих обстоятельствах:

- не подтверждено, что владелец Сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком Сертификате;

- установлено, что содержащийся в таком Сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном Сертификате ключа проверки электронной подписи;

- вступило в силу решение суда, которым, в частности, установлено, что Сертификат ключа проверки электронной подписи содержит недостоверную информацию.

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;

− уполномоченным представителем юридического лица (в случае изготовления сертификата для сотрудника ЮЛ) на основании заявления владельца Сертификата, подаваемого в форме документа на бумажном носителе;

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

Процедура рассмотрения запроса на аннулирование (отзыв) Сертификата

Запрос на аннулирование (отзыв) должен быть подан на бумажном носителе.

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.

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.

Структура Удостоверяющего центра

Центр сертификации

Центр сертификации (далее-ЦС) предназначен для: выпуска сертификатов Заявителям УЦ 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; ○ 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.

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.

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.

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 УЦ 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.

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.

Предоставление информации

Сторона, присоединяющаяся к Регламенту, предоставляет в Удостоверяющий центр следующие сведения и надлежащим образом заверенные копии документов, их подтверждающие:

Для юридических лиц:

- Паспорт владельца Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства) или нотариально заверенная копия указанного документа или надлежащим образом заверенный документ, содержащий сведения паспорта владельца Сертификата, с приложением копии указанного документа, в случае если владелец не является получателем Сертификата.
- Паспорт получателя Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства).
- СНИЛС владельца Сертификата, оригинал или нотариально заверенная копия указанного документа или надлежащим образом заверенный документ, содержащий сведения паспорта владельца Сертификата, с приложением копии указанного документа, в случае если владелец не является получателем Сертификата.
- Доверенность, подтверждающая полномочия владельца Сертификата ключа подписи (в случае, если владелец сертификата не имеет права действовать от имени юридического лица без доверенности) или надлежащим образом заверенная копия Приказа на владельца Сертификата на представление интересов юридического лица.
- Доверенность на получение сертификата ключа подписи (в случае, если Сертификат получает доверенное лицо, а не владелец Сертификата).
- Сведения об основном государственном регистрационном номере Заявителя УЦ или номер свидетельства о постановке на учет в налоговом органе Заявителя УЦ – иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или о идентификационном номере налогоплательщика Заявителя УЦ - иностранной организации (указывается Заявителем УЦ в заявлении, которое направляется посредством электронной системы подачи заявлений УЦ, необходимого для выпуска сертификата).

Для индивидуальных предпринимателей:

- паспорт владельца Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства) или нотариально заверенная копия указанного документа или надлежащим образом заверенный документ, содержащий сведения паспорта владельца Сертификата, с приложением копии указанного документа, в случае если владелец не является получателем Сертификата.
- Паспорт получателя Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства).
- СНИЛС владельца Сертификата, оригинал или нотариально заверенная копия указанного документа или надлежащим образом заверенный документ, содержащий сведения паспорта владельца Сертификата, с приложением копии указанного документа, в случае если владелец не является получателем Сертификата.
- Доверенность, подтверждающая полномочия владельца Сертификата ключа подписи (в случае, если владелец Сертификата не имеет права действовать от лица Индивидуального предпринимателя без доверенности) или надлежащим образом заверенная копия Приказа на владельца Сертификата на представление интересов Индивидуального предпринимателя.
- 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 УЦ в заявлении, которое направляется посредством электронной системы подачи заявлений УЦ, необходимого для выпуска сертификата).

Для физических лиц:

- Паспорт владельца Сертификата (страницы паспорта с разворотом с фотографией и последней отметкой о регистрации постоянного места жительства) или копия заверенная нотариально.
- СНИЛС владельца сертификата или копия заверенная нотариально копия.
- Идентификационный номер налогоплательщика или копия заверенная нотариально копия.
- Доверенность, нотариально заверенная, подтверждающая право действовать от имени Заявителя УЦ (в случае если физическое лицо не будет являться владельцем Сертификата).

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 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 от 06.04.2011 № 63-ФЗ «Об электронной подписи» (в случае необходимости).

Если Заявитель УЦ выступает в интересах третьих лиц, то, по требованию Удостоверяющего центра, представляет документы, подтверждающие такие полномочия.

Права и обязанности Сторон

Удостоверяющий центр обязан:

1. Предоставить пользователю Сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.
2. Использовать для создания ключа электронной подписи Удостоверяющего центра и формирования электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
3. 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.
4. Вносить в создаваемые Сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами.
5. Использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им Сертификатов ключей проверки электронной подписи и списков, отозванных (аннулированных) Сертификатов.
6. Обеспечить защиту ключа электронной подписи Удостоверяющего центра от несанкционированного доступа.

7. Организовать свою работу по московскому времени и синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

8. Обеспечить уникальность идентификационных данных пользователей Удостоверяющего центра, заносимых в Сертификаты ключей проверки электронной подписи.

9. Создать Сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра по заявлению на создание Сертификата, в соответствии с порядком, определенным в Регламенте.

10. Обеспечить уникальность серийных номеров создаваемых Сертификатов.

11. Обеспечить уникальность значений ключей проверки электронной подписи в созданных Сертификатах пользователей УЦ.

12. Обеспечить сохранение в тайне созданного ключа электронной подписи пользователя Удостоверяющего центра.

13. Прекратить (аннулировать), приостановить и возобновить действие Сертификата пользователя Удостоверяющего центра по соответствующему заявлению (Приложение №2, Приложение № 3 к Регламенту), в соответствии с порядком, определенным в Регламенте.

14. Прекратить действие Сертификата пользователя, если истек установленный срок, на который действие данного сертификата было приостановлено.

15. Прекратить действие Сертификата пользователя в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра.

16. 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.

17. Произвести регистрацию квалифицированного сертификата ЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ.

18. Публиковать актуальный список отозванных (аннулированных) Сертификатов на сайте Удостоверяющего центра.

19. Информировать в письменной форме Заявителей УЦ 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.

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

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

22. 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.

Заявители обязаны:

1. Предъявить документы, удостоверяющие личность Заявителя УЦ, доверенного лица Заявителя УЦ, Заявителя - физического лица в соответствии порядком предоставления информации Регламента.

2. 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.

3. Совершать действия, направленные на обеспечение безопасности и законности процесса выдачи Сертификата (в том числе с использованием различных технических средств).

Пользователи УЦ обязаны:

1. Обеспечивать конфиденциальность ключей электронных подписей.

2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

3. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие ограничения были установлены.

4. 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 № 2 к Регламенту).

5. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован или действие которого приостановлено.

Обязанности Участников электронного взаимодействия:

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

2. Использовать ЭП в соответствии с ограничениями, содержащимися в Сертификате ключа проверки этой электронной подписи.

3. Уведомлять Удостоверяющий центр, выдавший Сертификат, и иных участников электронного взаимодействия о нарушении конфиденциальности Ключа электронной подписи со дня получения информации о таком нарушении.

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

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

Права Удостоверяющего центра:

1. 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.

2. 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.

3. Отказать в выдаче Сертификата в случае невыполнения обязанностей, а также если услуга по созданию и выдаче Сертификата не оплачена в надлежащем порядке.

4. Отказать в создании сертификата ключа проверки электронной подписи пользователю Удостоверяющего центра в случае не предоставления и/или предоставления не надлежаще оформленных документов, необходимых для создания сертификата ключа проверки.

5. Отказать в аннулировании, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи пользователю Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления.

6. Отказать в аннулировании, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи пользователю Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату.

7. 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.

8. В одностороннем порядке прекратить действие сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра с обязательным его уведомлением и указанием обоснованных причин.

9. В установленном порядке приостановить действие Сертификата, а также восстановить действие ранее приостановленного Сертификата.

Права Пользователей Удостоверяющего центра:

1. Применять сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в сертификатах ключей проверки электронных подписей, созданных Удостоверяющим центром.

2. Применять список отозванных (аннулированных) сертификатов ключей проверки электронных подписей, созданный Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

3. Для хранения ключа электронной подписи применять ключевой носитель, поддерживаемый средством электронной подписи, определённым сертификатом ключа проверки электронной подписи, соответствующим ключу электронной подписи.

4. Получить копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Удостоверяющим центром.

5. Получить от Удостоверяющего центра инструкции по обеспечению безопасности использования электронной подписи и Средств электронной подписи.

6. Обратиться в Удостоверяющий центр с заявлениями на выполнение Удостоверяющим центром действий, установленных Регламентом.

Конфиденциальность

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

Типы конфиденциальной информации:

Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не депонирует и не архивирует ключи электронной подписи Пользователей Удостоверяющего центра.

Пароль, предоставляемый пользователю Удостоверяющего центра в процессе прохождения процедуры регистрации, считается конфиденциальной информацией.

Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной

рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.
Информация, хранящаяся в журналах аудита Удостоверяющего центра, считается конфиденциальной и не подлежит разглашению.
Отчетные материалы по выполненным проверкам деятельности Удостоверяющего центра являются конфиденциальными, за исключением заключения по результатам проверок, публикуемого в соответствии с Регламентом.

Типы информации, не являющейся конфиденциальной:

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.
Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.
Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.
Информация, содержащаяся в Регламенте, не считается конфиденциальной.

Архивное хранение

Архивированию подлежат следующая документированная информация:

- реестр сертификатов ключей проверки электронной подписи пользователей Удостоверяющего центра;
- сертификаты ключей проверки электронной подписи уполномоченного лица Удостоверяющего центра;
- журналы аудита программно-аппаратных средств обеспечения деятельности 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 № 2 к Регламенту);
- заявления о возобновлении действия сертификата ключа проверки электронной подписи (Форма –Приложение № 3 к Регламенту);
- внутренние документы Удостоверяющего центра.

Хранение документируемой информации

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

Уничтожение архивных документов

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

Публикация и ответственность за актуальность информации в репозитории

Репозиторий

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

Публикация информации

Публикации подлежит:

- сертификат Центра сертификации УЦ;
- список аннулированных сертификатов;
- политики применения сертификатов;
- регламент применения сертификатов (настоящий Регламент УЦ);
- шаблоны заявлений на выпуск сертификата;
- шаблон соглашения с клиентом;
- шаблон соглашения с пользователем;
- сведения об аттестации и аккредитации;
- сопутствующая информация, уведомления, обновления и исправления.

Время и частота публикаций

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

Управление доступом к репозиториям

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

ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Генерация и инсталляция ключевых пар

Генерация ключевых пар

Генерация ключевых пар может производиться Клиентом 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 Пользователю УЦ

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

Передача ключа проверки электронной подписи издателю сертификата

При создании запроса на сертификат Пользователем УЦ, он может передать ключ проверки электронной подписи в УЦ следующими способами:

- в составе запроса формата PKCS#10 по защищенному каналу связи, обеспечивающему аутентификацию клиента и целостность передаваемого запроса;

- в составе подписанного запроса формата PKCS#10; при этом запрос подписывается с применением ключа электронной подписи, соответствующего действующему сертификату Пользователя УЦ;

- на ключевом носителе лично сотруднику УЦ с предъявлением документов, удостоверяющих личность.

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).

Создание копий ключей электронной подписи на компьютере при использовании отчуждаемого носителя для хранения ключей недопустимо.

Контроль ключа электронной подписи несколькими лицами

Контроль ключа электронной подписи несколькими лицами недопустим.

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.

Структура сертификатов

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.

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;

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;

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 COC версии 2.

Расширения CRL и элементов CRL

- **Authority Key Identifier**

Идентификатор ключа Центра сертификации, которым подписан данный COC.

- **CRL Number**

Некритическое рекомендуемое расширение, содержащее порядковый номер COC.

- **Reason Code**

Некритическое рекомендуемое расширение элемента CRL, содержащее причину отзыва сертификата.

_____ «_____»
(полное название организации)

ИНН _____ ОКАТО _____
Юридический адрес:_____

ДОВЕРЕННОСТЬ

На получение сертификата ключа проверки электронной подписи в УЦ ООО «ВБЦ» за владельца сертификата ключа проверки электронной подписи

город _____ _____
(дата)

Организация _____ «_____»,

в лице _____,
(должность, Ф.И.О.)

действующего на основании _____,

настоящей доверенностью уполномочивает:

_____,
(должность, Ф.И.О.)

паспорт: серия _____ № _____ выдан _____ .

1. Предоставить в УЦ ООО «ВБЦ» документы, необходимые для формирования ключей ЭП и сертификата ключа проверки электронной подписи уполномоченного представителя.
2. Получить сформированные ключи ЭП и сертификат ключа проверки электронной подписи Пользователя УЦ ООО «ВБЦ».

Доверенность выдана сроком на 1(один) год и 3(три) месяца без права передоверия.

/_____/_____
(Ф.И.О. доверенного лица, подпись)

/_____/_____
(Ф.И.О. доверителя подпись)

_____/_____/_____
(Должность руководителя, Ф.И.О., подпись)

Приложение № 2 к Регламенту УЦ

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 № 3 к Регламенту УЦ

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

Руководство по обеспечению безопасности использования средств криптографической защиты информации

Пользователь 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.

Пользователю 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.

Пользователь 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.

Приложение № 5 к Регламенту УЦ

ЗАЯВЛЕНИЕ
на создание сертификата ключа электронной подписи представителю юридического лица

_____
(полное наименование организации, включая организационно-правовую форму)
в лице
_____
(должность, фамилия, имя, отчество)
действующего на основании
_____
просит создать квалифицированный сертификат ключа проверки электронной подписи

V включает СКЗИ "КриптоПро CSP")

Сокращенное наименование организации в соответствии с выпиской из ЕГРЮЛ	
Юридический адрес (в соответствии с выпиской из ЕГРЮЛ)	
Код региона/Наименование региона	
Фактический адрес	
ИНН КПП ОГРН	
Фамилия, Имя, Отчество физического лица, действующего от имени юридического лица	
Должность (не более 128 символов)	
Наименование подразделения (при наличии) (не более 64 символов)	
Адрес электронной почты	
Область применения	
Паспортные данные (серия, номер, кем выдан, дата выдачи)	
СНИЛС	- - -
Класс средств ЭП	КС1

Кодовое словосочетание:

В случае изготовления сертификата по инициативе работодателя, я так же подтверждаю свое согласие с его намерениями воспользоваться услугой ООО «ВБЦ» для выпуска сертификата на мое имя.

Физическое лицо, действующее
от имени юридического лица _____ _____
(подпись) (фамилия, инициалы)

Руководитель организации _____ _____
(подпись) М.П. (фамилия, инициалы)

«____»_____ 20____ г.

Приложение № 6 к Регламенту УЦ

ЗАЯВЛЕНИЕ
на создание сертификата ключа электронной подписи индивидуальному предпринимателю

_____
(фамилия, имя, отчество)

просит создать квалифицированный сертификат ключа проверки электронной подписи

V	включает СКЗИ "КриптоПро CSP")

Для выпуска сертификата сообщаю следующие данные:

Фактический адрес	
ИНН ОГРНИП	
Фамилия, Имя, Отчество физического лица	
Адрес электронной почты	
Область применения	
Паспортные данные (серия, номер, кем выдан, дата выдачи)	
СНИЛС физического лица	
Класс средств ЭП	КС1

Кодовое словосочетание:

_____ _____
(подпись) (ФИО)

«____»_____ 20____ г. М.П

Приложение № 7 к Регламенту УЦ

ЗАЯВЛЕНИЕ
на создание сертификата ключа электронной подписи физическому лицу

_____
(фамилия, имя, отчество)

просит создать квалифицированный сертификат ключа проверки электронной подписи

V	включая СКЗИ "КриптоПро CSP")

Для выпуска сертификата сообщаю следующие данные:

Адрес регистрации (в соответствии с паспортом)	
Код региона/Наименование региона	
Фактический адрес	
ИНН	
Фамилия, Имя, Отчество	
Адрес электронной почты	
Область применения	
Паспортные данные (серия, номер, кем выдан, дата выдачи)	
СНИЛС	- - -
Класс средств ЭП	КС1

Кодовое словосочетание:

«____»_____ 20____ г. _____ _____
(подпись) (ФИО)