УТВЕРЖДАЮ

Генеральный директор ОАО «ОЭП»

_____О.Г.Звонов

«01»июля 2015 г.

РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ЗАЩИЩЕННОЙ СЕТИ ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ОПЕРАТОР ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА»

Редакция № 1

Введен в действие Приказом №04Т от «01» июля 2015г.

г. Пенза

1 Сведения об Удостоверяющем центре

Удостоверяющий центр защищенной сети ОАО «Оператор электронного правительства» является корпоративным удостоверяющим центром и предназначен для обеспечения юридически значимого электронного документооборота и криптографической защиты информации при информационном взаимодействии организаций, участвующих в электронном документообороте и иных функций, связанных с использованием электронной подписи. Регламент Удостоверяющего центра защищенной сети ОАО «Оператор электронного правительства» создан с учетом следующих нормативных правовых документов:

1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных";

4. Гражданский Кодекс Российской Федерации от 30.11.1994 № 51-ФЗ (часть первая, ст. 160, 428, 434);

5. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

6. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

Удостоверяющий центр защищенной сети ОАО «Оператор электронного правительства» осуществляет свою деятельность на основании Лицензии ФСБ России ЛСЗ № 0005414 от 08 августа 2014 г. на право осуществления работ, предусмотренных пунктами 2, 3, 7, 8, 9, 11, 12, 13, 14, 15, 17, 18, 20, 21, 22, 23, 24, 25, 26, 27, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313

Реквизиты ОАО «ОЭП»:
Полное наименование:
Открытое акционерное общество «Оператор электронного правительства»
Юридический адрес: 440068 г. Пенза, ул. Центральная, д. 1В
Адрес для корреспонденции: 440068 г. Пенза, ул. Центральная, д. 1В
Банковские реквизиты:
Р/С 40702810548000035593
в Пензенском отделении №8624 ОАО «Сбербанк России» г. Пенза
БИК 045655635
к/с 30101810000000000635
ИНН: 5836646090
КПП: 583701001
ОГРН: 1115836002193

Код по ОКПО: 90698286

Контактные сведения:
тел. +7 (8412), 23-11-28
http://rosoperator.ru/

2 Термины и определения

Абонент защищенной сети ОАО «Оператор электронного правительства», абонент — владелец сертификата ключа проверки электронной подписи (далее — СКПЭП), включённый в список абонентских пунктов и абонентов защищенной сети ОАО «Оператор электронного правительства» и зарегистрированный хотя бы на одном из абонентских пунктов.

Абонентский пункт защищенной сети ОАО «Оператор электронного правительства», абонентский пункт (далее — АП) — компьютер, включённый в список абонентских пунктов и абонентов защищенной сети ОАО «Оператор электронного правительства», на котором зарегистрирован хотя бы один абонент, с установленными криптографическими средствами защиты информации – программным обеспечением (далее — ПО) ViPNet [Клиент], реализующими функции шифрования и электронной подписи.

Автоматизированное рабочее место (АРМ) ViPNet [Администратор] — аппаратно-программный комплекс (АПК), представляющий собой компьютер с установленным программным обеспечением (ПО) ViPNet [Центр управления сетью] и ViPNet [Удостоверяющий и Ключевой центр], установленный и эксплуатируемый Администратором Удостоверяющего центра защищенной сети ОАО «Оператор электронного правительства».

Администратор Удостоверяющего центра защищенной сети ОАО «Оператор электронного правительства» (Уполномоченное лицо Удостоверяющего центра) — ответственный сотрудник ОАО «Оператор электронного правительства», наделенный полномочиями по осуществлению действий по регистрации, управлению и заверению СКПЭП пользователей Удостоверяющего центра защищенной сети ОАО «Оператор электронного правительства» и списков отозванных сертификатов, изданных Удостоверяющим центром защищенной сети ОАО «Оператор электронного правительства», и уполномоченный расписываться собственноручной подписью в копиях СКПЭП, изданных Удостоверяющим центром защищенной сети ОАО «Оператор электронного правительства».

Владелец сертификата ключа подписи (Пользователь Удостоверяющего центра)— лицо, которому в установленном порядке Удостоверяющим центром защищенной сети ОАО «Оператор электронного правительства» выдан СКПЭП и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Доверенный способ передачи информации — способ передачи информации, принятый двумя или несколькими юридическими или физическими лицами на основе взаимной договоренности и обеспечивающий требуемую степень её защищенности.

Защищенная сеть ОАО «Оператор электронного правительства», защищенная сеть - это совокупность сетевых узлов (абонентских пунктов и координаторов), управляемая ОАО «Оператор электронного правительства» и защищаемая с помощью продуктов линейки ViPNet CUSTOM 3.2 (Инфотекс, г. Москва). Номер сети ViPNet 2982.

Заявитель – физическое лицо, юридическое лицо, индивидуальный предприниматель, обратившийся за получением квалифицированного сертификата

ключа проверки электронной подписи или иных услуг в Удостоверяющий центр защищенной сети ОАО «Оператор электронного правительства».

Издание сертификата означает, что запрос на сертификат подписывается текущим Администратором и, следовательно, становится сертификатом.

Исходная ключевая информация — совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

Ключ электронной подписи (КЭП) — уникальная последовательность символов предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (КПЭП) — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключевой дистрибутив — файл с расширением .DST, создаваемый ПО УКЦ для каждого абонента сетевого узла, в котором в зашифрованном виде на парольном ключе помещена необходимая адресная и ключевая информация (или исходная ключевая информация) для обеспечения первичного запуска на компьютере ПО ViPNet [Клиент] или ViPNet [Координатор].

Ключевые документы — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

Ключевая информация — специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой носитель — физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.).

Компрометация ключа — утрата доверия к тому, что используемые ключи шифрования и/или КЭП обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Конфликтная ситуация — ситуация, при которой у участника системы электронного документооборота с применением ЭП возникает необходимость разрешения вопросов признания или не признания авторства и/или подлинности электронных документов, обработанных с помощью средств ЭП.

Координатор — компьютер с установленным ПО ViPNet [Координатор], который устанавливается на границе ЛВС и обеспечивает:

- включение в защищённую сеть открытых и защищенных компьютеров, находящихся в этой ЛВС, независимо от типа адреса, выделяемого им;

- разделение и защиту сетей от сетевых атак;

- оповещение администратора удостоверяющего центра о состоянии других сетевых узлов, связанных с ним.

Копия сертификата ключа проверки электронной подписи - документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра защищенной сети ОАО «Оператор электронного правительства» и заверенный печатью Удостоверяющего центра, а также владельцем СКПЭП. Содержательная часть Копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи.

Криптосредство — шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) — шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Криптографический ключ (криптоключ) — совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Кросс-сертификация — комплекс организационно-технических мероприятий, предпринимаемых удостоверяющими центрами для установления взаимных доверенных отношений. Кросс-сертификация между удостоверяющими центрами обеспечивает прозрачное взаимодействие между пользователями этих УЦ.

Кросс-сертификат — СКПЭП, владельцем которого является Уполномоченное лицо одного удостоверяющего центра, а издателем – Уполномоченное лицо другого удостоверяющего центра.

Аннулирование сертификата — признание сертификата недействительным в период его действия.

Плановая смена КЭП — смена КЭП с установленной периодичностью, не вызванная компрометацией криптоключей.

Подтверждение подлинности электронной подписи в электронном документе — положительный результат проверки средствами абонентского пункта с использованием КПЭП принадлежности ЭП в электронном документе владельцу СКПЭП и отсутствия искажений в подписанном данной ЭП электронном документе.

Реестр Удостоверяющего центра — набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений о присоединении к регламенту Удостоверяющего центра;

- реестр заявлений на изготовление СКПЭП;

- реестр выдачи СКПЭП;

Сеть VipNet — это совокупность сетевых узлов (абонентских пунктов и координаторов).

Сертификат ключа проверки электронной подписи (СКПЭП) — электронный документ, выданный удостоверяющим центром либо доверенным лицом

удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. В сети ViPNet сертификат выдается Удостоверяющим и Ключевым центром и заверяется ЭП Администратора. Сертификат включает имя издателя сертификата, описание владельца сертификата, его открытый ключ, период действия сертификата, а также дополнительные параметры. ЭП Администратора, заверяющая содержимое каждого сертификата, обеспечивает подлинность и целостность указанной в нем информации, включая описание владельца и его КПЭП. Спецификация содержимого и формат сертификата в сети ViPNet соответствует стандарту X.509 версии 3 и Федеральному закону от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Список аннулированных сертификатов – электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров СКПЭП, которые на определенный момент времени были аннулированы.

Средства удостоверяющего центра — программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра, в частности включают в себя:

ПО ViPNet [Клиент] — обеспечивает надежную защиту компьютера от несанкционированного доступа к различным информационным и аппаратным ресурсам на нем при работе компьютера в локальных или глобальных сетях, например, Интернет, в том числе от сетевых атак, и установление криптографически защищенных соединений при взаимодействии с другими узлами защищенной сети ОАО «Оператор электронного правительства», а также возможность гарантированной доставки подписанных ЭП сообщений (файлов) по назначению с автоматическим подтверждением доставки и прочтения документов;

ПО ViPNet [Центр управления сетью] (ЦУС) — предназначено для создания и управления конфигурацией виртуальной сети на базе распределенной системы персональных и межсетевых экранов технологии ViPNet, обеспечивающей защиту функционирования компьютеров и передаваемой информации в защищенной сети ОАО «Оператор электронного правительства», и решает следующие основные задачи:

- построение инфраструктуры виртуальной сети (узлы защищенной сети и - связи между ними, включая межсетевые);

- изменение конфигурации сети;

- формирование и рассылка защищенных адресных справочников, защищенных таблиц маршрутизации;

- формирование информации о ключевых связях абонентов для Ключевого Центра;

- определение прав доступа к ресурсам каждого абонента;

ПО ViPNet [Удостоверяющий и Ключевой центр] (УКЦ) — состоит из Удостоверяющего центра, практически реализующего выполнение функций УЦ ViPNet-сети №2982, связанных с изданием, заверением, отзывом и хранением сертификатов ключей подписи, а также других функций, предусмотренных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», и

Ключевого центра, обеспечивающего формирование и обновление ключевой информации для взаимодействия между узлами защищенной сети и абонентами в соответствии с заданными связями.

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.

Удостоверяющий центр (УЦ) — юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Удостоверяющий центр защищенной сети ОАО «Оператор электронного правительства» — совокупность инфраструктуры программных и технических средств, администраторов и персонала ОАО «Оператор электронного правительства», обеспечивающих деятельность по изготовлению и управлению СКПЭП пользователей УЦ ОАО «Оператор электронного правительства» и выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи».

Узел защищенной сети (сетевой узел) — это функционирующий абонентский пункт или координатор.

Уполномоченное лицо УЦ защищенной сети ОАО «Оператор электронного правительства» — физическое лицо, являющееся сотрудником ОАО «Оператор электронного правительства», наделенное полномочиями по заверению СКПЭП пользователей Удостоверяющего центра и списков отозванных сертификатов.

Участники электронного взаимодействия — организации, присоединившиеся к Регламенту Удостоверяющего центра защищенной сети ОАО «Оператор электронного правительства», взаимодействующие с ОАО «Оператор электронного правительства» в целях выполнения функций, предусмотренных действующим законодательством РФ и осуществляющие защищенный обмен информацией в электронной форме.

Электронный документ — документ, информация в котором представлена в электронно-цифровой форме.

Электронная подпись (ЭП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3 Статус регламента

3.1 Регламент Удостоверяющего центра защищенной сети ОАО «ОЭП», именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации.

3.2 Настоящий Регламент является договором присоединения на основании ст. 428 Гражданского кодекса Российской Федерации.

3.3 Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра защищенной сети ОАО «ОЭП», включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

3.4 Целью настоящего Регламента является создание условий для организации защищенного сетевого взаимодействия информационных систем участников и правовых условий использования электронной подписи, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

3.5 Опубликование Регламента, включая распространение его текста в глобальной компьютерной сети Интернет по адресу http://rosoperator.ru/info/docs/reglament_vipnet.pdf, должно рассматриваться всеми заинтересованными лицами как публичное предложение (оферта) со стороны ОАО «ОЭП» заключить договор на предоставление услуг, существенные условия которого зафиксированы в настоящем Регламенте.

3.6 Помимо размещения Регламента на сайте, в офисе ОАО «ОЭП» хранится экземпляр Регламента с приложениями, прошитый и заверенный печатью и подписью Генерального директора ОАО «ОЭП». Совершая акцепт настоящего Регламента, Заявитель соглашается с тем, что в случае возникновения спора в качестве доказательства принимается текст Регламента и приложений к нему, который прошит, пронумерован, скреплен подписью Генерального директора и печатью ОАО «ОЭП».

3.7 Удостоверяющий центр защищенной сети ОАО «Оператор электронного правительства» создан и работает для организации защищенного электронного взаимодействия с помощью сети ViPNet №2982. При необходимости устанавливается межсетевое взаимодействие с защищёнными сетями учреждений и организаций, с которыми взаимодействует ОАО «Оператор электронного правительства» или абоненты защищенной сети ОАО «ОЭП».

4 Общие положения

4.1 Присоединение к Регламенту

4.1.1 Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления Заявителем в ОАО «ОЭП» Заявления о присоединении к Регламенту. Форма Заявления о присоединении к Регламенту приведена в Приложении №1 к настоящему Регламенту.

4.1.2 С момента регистрации Заявления о присоединении к Регламенту в Удостоверяющем центре защищенной сети ОАО «ОЭП» лицо, подавшее Заявление о присоединении к Регламенту, считается присоединившемся к Регламенту и является Стороной Регламента.

4.1.3 Удостоверяющий центр защищенной сети ОАО «ОЭП» вправе отказать любому лицу в приеме и регистрации Заявления о присоединении к Регламенту с указанием причин отказа.

4.1.4 Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении к регламенту в Удостоверяющем центре защищенной сети ОАО «ОЭП». Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

4.1.5 После присоединения к Регламенту Удостоверяющий центр защищенной сети ОАО «ОЭП» и Сторона, присоединившаяся к Регламенту, считаются вступившими в соответствующие договорные отношения на неопределённый срок.

4.2 Порядок расторжения договорных отношений

3.9.1 Договорные отношения могут быть прекращены по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- нарушения одной из Сторон условий настоящего Регламента.

3.9.2 В случае расторжения договорных отношений инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за 30 (тридцать) календарных дней до даты расторжения договорных отношений. Договорные отношения считаются расторгнутым после выполнения Сторонами своих обязательств и проведения взаиморасчетов согласно условиям Регламента.

3.9.3 Прекращение действия Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

4.3. Изменения (дополнения) Регламента

3.10.1 Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром защищенной сети ОАО «ОЭП» в одностороннем порядке.

3.10.2 Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром защищенной сети ОАО «ОЭП» путем обязательного размещения указанных изменений (дополнений) в сети Интернет

3.10.3 Все изменения (дополнения), вносимые Удостоверяющим защищенной сети ОАО «ОЭП» в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении 7 (семи) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра защищенной сети ОАО «ОЭП»

3.10.4 Все изменения (дополнения), вносимые Удостоверяющим центром защищенной сети ОАО «ОЭП» в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

3.10.5 Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренным настоящим Регламентом.

3.10.6 Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

4.4 Применение Регламента

3.11.1 Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

3.11.2 В случае противоречия и/или расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

3.11.3 В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

5 Предоставление информации

5.1 Удостоверяющий центр защищенной сети ОАО «ОЭП» вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить Удостоверяющему центру защищенной сети ОАО «ОЭП» следующий перечень документов, необходимых для подтверждения сведений, заносимых в сертификат (далее – Заявительные документы):

Для юридических лиц:

- оригинал или нотариально заверенную копию выписки из Единого государственного реестра юридических лиц, полученную не ранее чем за 3 месяца до ее представления;
- надлежащим образом оформленное Заявление на создание сертификата ключа проверки электронной подписи (с указанием в качестве владельца сертификата ключа проверки электронной подписи уполномоченного представителя - по форме Приложения №2);
- если сертификат изготавливается на имя Уполномоченного представителя: доверенность, подтверждающую полномочия Уполномоченного представителя, оформленную по форме Приложения №3 настоящего Регламента, подписанную руководителем или иным лицом, уполномоченным на это учредительными документами Заявителя - юридического лица и заверенную печатью Заявителя - юридического лица;
- заверенную надлежащим образом копию второй и третьей страницы паспорта гражданина Российской Федерации, на чье имя изготавливается сертификат;
- если документы для изготовления сертификата предоставляет и / или получает не Заявитель, а его Доверенное лицо: доверенность на предоставление документов и / или получение ключевого документа и сертификата за Заявителя, по форме Приложения №4, подписанную руководителем или иным лицом, уполномоченным на это учредительными документами Заявителя - юридического лица и заверенную печатью Заявителя - юридического лица, с одновременным предъявлением паспорта гражданина РФ Доверенным лицом;

5.2 Комплект документов, необходимых для выпуска сертификата может быть изменён в зависимости от типа сертификата.

5.3 Удостоверяющий центр защищенной сети ОАО «ОЭП» оставляет за собой право запросить у Стороны, присоединившейся к Регламенту, дополнительные документы.

5.4 В случае отсутствия у лица, на чье имя изготовляется сертификат, паспорта гражданина Российской Федерации, допускается предоставление иного документа, удостоверяющего личность в соответствии с законодательством Российской Федерации.

5.5 В целях настоящего документа под надлежащим образом заверенными копиями документов понимаются копии:

- для юридических лиц – заверенные нотариусом или лицом, действующим от имени юридического лица без доверенности и печатью юридического лица;

5.6 В случае представления Заявителем только оригиналов Заявительных документов уполномоченный сотрудник Удостоверяющего центра защищенной сети ОАО «ОЭП» осуществляет их копирование и заверение копий.

5.7 Сторона, присоединившаяся к Регламенту, несет ответственность за достоверность сведений, предоставленных в Удостоверяющий центр защищенной сети ОАО «ОЭП».

5.8 Копии документов, подтверждающие сведения, внесенные в сертификат, подлежат хранению в Удостоверяющем центре.

6 Права и обязанности сторон

6.1 Удостоверяющий центр защищенной сети ОАО «ОЭП» обязан:

6.1.1 Предоставить Владельцу сертификата ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП» СКПЭП Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП» (обеспечить доступность корневых сертификатов УЦ защищенной сети ОАО «ОЭП»).

6.1.2 Использовать КЭП Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП» только для подписи издаваемых им СКПЭП и списков аннулированных сертификатов.

6.1.3 Принимать меры по защите КЭП Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП» от несанкционированного доступа.

6.1.4 Организовывать свою работу по UTC (всемирное координированное время) с учётом часового пояса города Москвы. Удостоверяющий центр защищенной сети ОАО «ОЭП» обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

6.1.5 Обеспечивать регистрацию Заявителей в Удостоверяющем центре защищенной сети ОАО «ОЭП» в соответствии со сведениями полученными из документов (заявление на присоединение к Регламенту, заявление на изготовление СКПЭП, доверенности и т.д.), предоставляемых Заявителем при регистрации в соответствии с порядком, определенным в настоящем Регламенте.

6.1.6 Обеспечивать занесение регистрационной информации Заявителей Удостоверяющего центра защищенной сети ОАО «ОЭП» в Реестр Удостоверяющего центра и обеспечивать уникальность регистрационной информации всех зарегистрированных в Удостоверяющем центре защищенной сети ОАО «ОЭП» лиц, используемой для идентификации владельцев СКПЭП.

6.1.7 Изготавливать сертификат Владельца сертификата ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП» по заявлению на изготовление сертификата в соответствии с порядком, определенным в настоящем Регламенте.

6.1.8 Обеспечивать уникальность серийных номеров изготавливаемых СКПЭП.

6.1.9 Обеспечивать уникальность значений ключей проверки подписи в изготовленных сертификатах Владельцев ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП».

6.1.10 Обеспечивать сохранение в тайне изготовленного КЭП (или исходной ключевой информации) Владельца сертификата ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП».

6.1.11 Аннулировать сертификат Владельца ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП» по соответствующему заявлению на аннулирование СКПЭП в соответствии с порядком, определенным настоящим Регламентом.

6.1.12 Аннулировать сертификат Владельца ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП» в случае компрометации КЭП

Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП», с использованием которого был издан СКПЭП.

6.1.13 Официально уведомлять об аннулировании действия СКПЭП всех Владельцев сертификатов ключа подписи, зарегистрированных в Удостоверяющем центре защищенной сети ОАО «ОЭП», путем публикации списка аннулированных сертификатов на странице в сети Интернет по адресу: http://oep-penza.ru. Официальным уведомлением о факте отзыва СКПЭП является опубликование первого (наиболее раннего) списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате, и изданного не ранее времени наступления произошедшего случая.

6.1.14 Публиковать актуальный список аннулированных сертификатов. Период публикации актуального списка аннулированных сертификатов в рабочее время Удостоверяющего центра защищенной сети ОАО «ОЭП» – 3 (три) месяца.

6.2 Удостоверяющий центр защищенной сети ОАО «ОЭП» имеет право:

6.2.1 Отказать Заявителю в регистрации в Удостоверяющем центре защищенной сети ОАО «ОЭП» в случае ненадлежащего оформления необходимых регистрационных документов, представления документов не в полном объёме, предоставление документов, подлинность которых вызывает сомнение.

6.2.2 Отказать Заявителю в изготовлении СКПЭП Удостоверяющего центра защищенной сети ОАО «ОЭП» в случае ненадлежащего оформления соответствующего заявления на изготовление СКПЭП.

6.2.3 Отказать в аннулировании СКПЭП Удостоверяющего центра защищенной сети ОАО «ОЭП» в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв) СКПЭП.

6.2.4 Отказать в аннулировании СКПЭП Удостоверяющего центра защищенной сети ОАО «ОЭП» в случае, если истёк установленный срок действия КЭП, с использованием которого был издан СКПЭП.

6.2.5 Отказать в изготовлении СКПЭП Удостоверяющего центра защищенной сети ОАО «ОЭП» в случае, если использованное Владельцем сертификата ключа подписи Удостоверяющего центра защищенной сети ОАО «ОЭП» для формирования запроса на СКПЭП средство криптографической защиты информации (средство электронной подписи) не поддерживается Удостоверяющим центром защищенной сети ОАО «ОЭП».

6.3 Сторона, присоединившаяся к Регламенту, обязана:

6.3.1 Известить Удостоверяющий центр защищенной сети ОАО «ОЭП» об изменениях в Заявительных документах, и по требованию Удостоверяющего центра сети защищенного электронного документооборота предоставить их в течение 5 (пяти) рабочих дней с даты регистрации изменений.

6.3.2 С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в 7 (семь) календарных дней обращаться на сайт Удостоверяющего центра защищенной сети ОАО «ОЭП» за сведениями об изменениях и дополнениях в Регламент.

6.4 Сторона, присоединившаяся к Регламенту, имеет право:

6.4.1 Обращаться установленным порядком в Удостоверяющий центр защищенной сети ОАО «ОЭП» с заявлением на изготовление СКПЭП.

6.4.2 Обращаться установленным порядком в Удостоверяющий центр защищенной сети ОАО «ОЭП» с заявлением на аннулирование СКПЭП в течение срока действия соответствующего КЭП.

6.5 Владелец сертификата обязан:

6.5.1 Хранить в тайне КЭП (ключевой носитель), принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

6.5.2 Применять для формирования ЭП только действующий КЭП.

6.5.3 Не применять КЭП, если стало известно, что этот ключ используется или использовался ранее другими лицами.

6.5.4 Немедленно обращаться в Удостоверяющий центр защищенной сети ОАО «ОЭП» с заявлением на аннулирование СКПЭП в случае потери, раскрытия, искажения личного КЭП, а также, в случае если стало известно, что этот ключ используется или использовался ранее другими лицами.

6.5.5 Не использовать КЭП, связанный с СКПЭП, заявление на аннулирование которого подано на рассмотрение Уполномоченному лицу Удостоверяющего центра защищенной сети ОАО «ОЭП», в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата по момент времени аннулирования сертификата, либо отказе в аннулировании.

6.5.6 Не использовать КЭП, связанный с СКПЭП, который аннулирован.

6.5.7 Не использовать КЭП до предоставления Удостоверяющему центру защищенной сети ОАО «ОЭП» подписанной копии СКПЭП, соответствующего данному КЭП.

6.6 Владелец сертификата имеет право:

6.6.1 Применять СКПЭП Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП» для проверки электронной подписи Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП» в СКПЭП, изготовленных Удостоверяющим центром защищенной сети ОАО «ОЭП».

6.6.2 Применять список отозванных СКПЭП, изготовленный Удостоверяющим центром защищенной сети ОАО «ОЭП», для установления статуса СКПЭП, изготовленных Удостоверяющим центром защищенной сети ОАО «ОЭП».

6.6.3 Для хранения КЭП применять сертифицированный носитель, поддерживаемый средством электронной подписи и Удостоверяющим центром защищенной сети ОАО «ОЭП».

6.6.4 Обращаться в Удостоверяющий центр защищенной сети ОАО «ОЭП» с заявлением на изготовление СКПЭП.

6.6.5 Обращаться установленным порядком в Удостоверяющий центр защищенной сети ОАО «ОЭП» с заявлением на аннулирование (отзыв) СКПЭП, владельцем которого он является в течение срока действия соответствующего КЭП.

6.6.6 Обращаться в Удостоверяющий центр защищенной сети ОАО «ОЭП» за получением информации о статусе СКПЭП и их действительности на определенный момент времени.

7 Вознаграждение Удостоверяющего центра защищенной сети ОАО «ОЭП»

7.1 Удостоверяющий Центр защищенной сети ОАО «ОЭП» осуществляет свою деятельность на платной основе.

7.2 Стоимость, сроки и порядок расчетов за предоставляемые услуги Удостоверяющего центра защищенной сети ОАО «ОЭП» регулируются договором между ОАО «ОЭП» и Заявителем.

7.3 Оплата осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на расчетный счет или иным способом, предусмотренным законодательством Российской Федерации.

7.4 Создание сертификатов в связи с внеплановой сменой ключей Владельцев сертификатов, связанной с нарушением конфиденциальности ключей электронной подписи Удостоверяющего центра защищенной сети ОАО «ОЭП», осуществляется Удостоверяющим центром защищенной сети ОАО «ОЭП» безвозмездно.

7.5 Удостоверяющий центр защищенной сети ОАО «ОЭП» выполняет аннулирование сертификатов, содержащихся в Реестре сертификатов безвозмездно.

8 Ответственность сторон

8.1 За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

8.2 Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

8.3 Удостоверяющий центр защищенной сети ОАО «ОЭП» не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр защищенной сети ОАО «ОЭП» обоснованно полагался на сведения, указанные в документах, предоставленных в соответствии с п.5.1 настоящего Регламента.

8.4 Удостоверяющий центр защищенной сети ОАО «ОЭП» несет ответственность за убытки при использовании созданного Удостоверяющим центром защищенной сети ОАО «ОЭП» ключа электронной подписи и сертификата ключа проверки электронной подписи в том случае, если данные убытки возникли по причине нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра защищенной сети ОАО «ОЭП».

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

9 Разрешение споров

9.1 Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр защищенной сети ОАО «ОЭП» и Сторона, присоединившаяся к Регламенту.

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

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

9.4 Сторона, получившая от другой Стороны претензию, обязана в течение 30 (тридцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

9.5 Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в порядке, установленном действующим законодательством Российской Федерации.

10 Порядок предоставления и пользования услугами Удостоверяющего центра защищенной сети ОАО «ОЭП»

10.1 Регистрация пользователей в качестве абонентов защищенной сети ОАО «Оператор электронного правительства», Изготовление ключей электронной подписи и сертификата

10.1.1 Удостоверяющий центр защищенной сети ОАО «ОЭП» осуществляет регистрацию абонентских пунктов и абонентов защищенной сети ОАО «ОЭП» в качестве узлов и абонентов сети VipNet №2982, а также осуществляет изготовление СКПЭП уполномоченным представителям юридических лиц, участников электронного взаимодействия, только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с пунктом 4.1 настоящего Регламента.

10.1.2 Регистрация Уполномоченного представителя юридического лица в качестве Пользователя УЦ защищенной сети ОАО «ОЭП» осуществляется на основании предоставления в УЦ защищенной сети ОАО «ОЭП» следующих документов:

заявления на присоединение к Регламенту (Приложение №1);

заявления на изготовление СКПЭП (Приложение №2);

других необходимых документов в соответствии с пунктом 5.1 настоящего Регламента.

Предоставление документов для регистрации пользователя и изготовления СКПЭП в Удостоверяющем центре защищенной сети ОАО «ОЭП» может быть осуществлено уполномоченным представителем Стороны, присоединившейся к Регламенту, на основании доверенности на регистрацию соответствующего пользователя, составленной по форме Приложения №3 настоящего Регламента.

10.1.3 Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» на основе предоставленных документов проводит следующие действия:

- выполняет процедуру идентификации лица, проходящего процедуру регистрации, путём установления личности (по документу, удостоверяющему личность);

- в случае положительной идентификации лица, проходящего процедуру регистрации, Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» принимает документы и осуществляет их проверку;

- проверяет сведения указанные в заявлениях на присоединение к регламенту и изготовление СКПЭП на предмет соответствия данным, содержащимся в документах их подтверждающих;

10.1.4 В случае нахождения недостоверных или ошибочных сведений, заявление на изготовления СКПЭП вместе с приложениями возвращается заявителю с указанием причины отказа Уполномоченным лицом Удостоверяющего центра защищенной сети ОАО «ОЭП»;

10.1.5 В случае отсутствия ошибок, Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП»:

- заносит сведения из заявления на присоединение к Регламенту и из заявления на изготовление СКПЭП в соответствующие журналы;

- на основании заявления на создание генерирует исходную ключевую информацию, изготавливает для неё СКПЭП;

- заносит сведения в журнал учёта выдачи дистрибутивов ключей;

- заносит сведения об изданном СКПЭП в реестр сертификатов;

- информирует Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП» о готовности.

10.1.6 Ключевой дистрибутив вместе с паролем доступа к нему, резервным набором персональных ключей и эксплуатационно-технической документацией ПО ViPNet [Клиент] передается лично абоненту или его доверенному лицу по доверенности (Приложение №3) под роспись в журнале учёта выдачи дистрибутивов ключей.

10.1.7 Установка ПО ViPNet [Клиент] на абонентские пункты производится с использованием выданных ключевых дистрибутивов пользователем Удостоверяющего центра защищенной сети ОАО «ОЭП» самостоятельно.

10.2 Изготовление и получение КЭП и СКПЭП при плановой смене ключей Пользователя Удостоверяющего центра

10.2.1 Владельцы сертификатов ключей подписи обязаны производить периодическую (плановую) замену используемого КЭП. Обновление СКПЭП и КЭП, который соответствует данному СКПЭП, требуется в следующих случаях:

- истекает срок действия СКПЭП;

- истекает срок действия КЭП;

- требуется получить СКПЭП, содержащий дополнительные атрибуты;

10.2.2 Замена КЭП осуществляется в обязательном порядке, если изменились данные, указанные в СКПЭП. При этом владелец сертификата обязан заблаговременно известить Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» об изменении данных и согласовать с ним дату и порядок смены КЭП.

10.2.3 Плановая смена ключей Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП» осуществляется один раз в год.

10.3 Смена СКПЭП и КЭП по истечению действия КЭП:

10.3.1 Пользователь УЦ заблаговременно со своего рабочего места в ПО ViPNet [Клиент] формирует новый КЭП и отправляет электронный запрос на формирование СКПЭП, без необходимости прибытия в УЦ.

10.3.2 Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» проверяет на корректность и достоверность сведения, указанные в запросе. В случае выявления недостоверных или ошибочных сведений, Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» отклоняет запрос и направляет уведомление абоненту посредством ПО Vipnet [Деловая почта] с указанием причины отклонения.

10.3.3 В случае, если в поступившем запросе нет ошибок, Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» регистрирует в

журнале учёта заявлений запрос, генерирует СКПЭП, информирует абонента о готовности СКПЭП.

10.3.4 Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» заносит в реестр сертификатов сведения о выданном СКПЭП и отправляет СКПЭП на абонентский пункт посредством ПО Vipnet [Администратор].

10.3.5 Пользователь УЦ самостоятельно производит установку и ввод в действие новых СКПЭП и КЭП на своем рабочем месте в ПО ViPNet [Клиент].

10.4 Смена ключей подписи при компрометации

10.4.1 Пользователь Удостоверяющего центра защищенной сети ОАО «ОЭП» информирует по средствам ПО Vipnet [Деловая почта] Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» о компрометации КЭП.

10.4.2 Пользователь Удостоверяющего центра защищенной сети ОАО «ОЭП» приносит в УЦ заявление на отзыв сертификата (Приложение №5) и получает новый ключевой дистрибутив для первичной инициализации АП.

10.4.3 Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» должно осуществлять изготовление СКПЭП Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП» по возможности в день получения электронного запроса, но не позднее дня истечения срока действия действующего КЭП.

10.5 Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП»

10.5.1 Удостоверяющий центр аннулирует (отзывает) СКПЭП Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП» в следующих случаях:

- в случае прекращения действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту;

- в случае отзыва доверенности Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП» на право действия от имени организации;

- по заявлению Пользователя Удостоверяющего центра защищенной сети ОАО «ОЭП»;

- при компрометации КЭП Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП».

10.5.2 Аннулирование (отзыв) СКПЭП Пользователя УЦ по заявлению его владельца:

Пользователь Удостоверяющего центра защищенной сети ОАО «ОЭП» предоставляет в Удостоверяющий центр защищенной сети ОАО «ОЭП» заявление на отзыв сертификата по форме Приложения №5.

Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» проверяет корректность заполнения заявления, в случае предоставления некорректных сведений отклоняет заявление на аннулирование (отзыв) сертификата и сообщает пользователю об отклонении с указанием причины.

В случае, если ошибок в заявлении на отзыв сертификата нет, Уполномоченное лицо Удостоверяющего центра защищенной сети ОАО «ОЭП» аннулирует (отзывает) СКПЭП Пользователя УЦ и выпускает список аннулированных сертификатов.

10.6 Конфиденциальность информации

10.6.1 Типы конфиденциальной информации

Ключ электронной подписи является конфиденциальной информацией лица, являющегося Владельцем соответствующего сертификата. Удостоверяющий центр защищенной сети ОАО «ОЭП» не осуществляет хранение ключей электронной подписи Владельцев сертификатов.

Персональная и корпоративная информация о Владельцах сертификатов, содержащаяся в Реестре сертификатов, не подлежащая непосредственной рассылке в качестве части сертификата, считается конфиденциальной.

10.6.2 Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией. Открытая информация может публиковаться по решению Удостоверяющего центра защищенной сети ОАО «ОЭП». Место, способ и время публикации открытой информации определяется Удостоверяющим центром защищенной сети ОАО «ОЭП».

Информация, включаемая в сертификаты и списки аннулированных сертификатов, создаваемые Удостоверяющим центром защищенной сети ОАО «ОЭП», не считается конфиденциальной.

Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, создаваемые Удостоверяющим центром защищенной сети ОАО «ОЭП», относятся к общедоступным персональным данным.

Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

11 Признание равнозначности электронной подписи и собственноручной подписи

11.1 Электронный документ, подписанный электронной подписью и полученный абонентом защищенной сети ОАО «ОЭП» с использованием средств абонентского пункта, на основании Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и настоящего Регламента признаётся эквивалентным такому же документу на бумажном носителе, заверенному собственноручной подписью должностных лиц учреждения, имеющих право подписи данного документа, от имени которого получен документ, и печатью соответствующего юридического лица, при условии соблюдения условий ст.6 и ст.9 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

11.2 При одновременном наличии электронного документа, подлинность электронной подписи которого подтверждается с помощью средств абонентского пункта, и эквивалентного ему документа на бумажном носителе, заверенного собственноручной подписью и печатью, подлинником документа считается электронный документ, а документ на бумажном носителе — его бумажной копией.

11.3 Стороны признают, что:

11.3.1 Применяемые для защиты сетевых соединений сертифицированные средства криптографической защиты информации обеспечивают аутентификацию, необходимый уровень конфиденциальности и целостности информации, защищаемой с применением этих средств, и достаточны для осуществления Сторонами защищенного обмена электронными документами по общедоступным каналам связи (в том числе сети Интернет) при условии использования нескомпрометированных ключей электронной подписи.

11.3.2 Электронная подпись признается равнозначной собственноручной подписи владельца сертификата, если соблюдены следующие условия:

- сертификат Пользователя создан с использованием сертификата Уполномоченного лица Удостоверяющего центра защищенной сети ОАО «ОЭП», сертификат которого действителен;

- сертификат Пользователя действителен на момент подписания электронного документа или на момент проверки действительности;

- имеется положительный результат проверки принадлежности Владельцу, подтверждено отсутствие изменений, внесенных в документ после его подписания;

11.3.3 Удостоверенные корректными электронными подписями электронные документы подтверждают Сторонам при обмене электронными документами:

- аутентификацию участников электронного обмена документами в процессе их взаимодействия;

- контроль целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия;

- конфиденциальность информации, представленной в электронном виде, передаваемой в процессе взаимодействия.

Список приложений

Приложение №1. Форма заявления о присоединении к Регламенту Удостоверяющего центра для юридических лиц.

Приложение №2. Форма заявления на создание сертификата ключа проверки электронной подписи для юридических лиц.

Приложение №3. Форма доверенности Пользователя Удостоверяющего центра.

Приложение №4. Форма доверенности на получение ключевых документов, сертификатов ключей проверки электронной подписи за Владельца сертификата в Удостоверяющем центре ОАО «ОЭП» (материальных ценностей) для юридических лиц.

Приложение №5. Форма заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи для юридических лиц.

Приложение №6. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Приложение № 1
Форма заявления о присоединении к Регламенту
Удостоверяющего центра защищенной сети

Заявление о присоединении к Регламенту Удостоверяющего центра защищенной сети ОАО «ОЭП»

_____
(наименование организации, включая организационно-правовую форму, ОГРН, ИНН)
в лице_____,
(должность, фамилия, имя, отчество)
действующего на основании_____

в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра защищенной сети ОАО «ОЭП», условия которого определены ОАО «ОЭП» и опубликованы на сайте Удостоверяющего центра защищенной сети ОАО «ОЭП» по адресу http://rosoperator.ru/info/docs/reglament_vipnet.pdf

С Регламентом Удостоверяющего центра защищенной сети ОАО «ОЭП» и приложениями к нему ознакомлен (-а) и обязуюсь соблюдать все положения указанного документа.

_____ _____ /_____ /
(должность руководителя организации) (подпись) (Ф.И.О.)

«____» _____ 201__года

Печать организации

_____

(заполняется сотрудником Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту зарегистрировано в реестре Удостоверяющего центра защищенной сети ОАО «ОЭП».

Регистрационный № ОКЗ-06-08-_____ от «_____» _____ 201___ г

Уполномоченный сотрудник
Удостоверяющего центра защищенной сети ОАО «ОЭП» _____ /_____ /
(подпись) (Ф.И.О.)

М.П.

Приложение № 2
Форма заявления на создание сертификата ключа
проверки электронной подписи для юридических лиц

Заявление зарегистрировано в УЦ под № ОКЗ-06-09-_____
«_____»_____201__г.

Заявление
на создание сертификата ключа проверки электронной подписи

_____
(полное наименование организации, включая организационно-правовую форму)
в лице_____
(должность, фамилия, имя, отчество) ,
действующего на основании__ _____ , просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи на предоставленный ключевой носитель для своего уполномоченного представителя:

_____
(фамилия, имя, отчество уполномоченного представителя)
В сертификат ключа проверки электронной подписи прошу занести следующие данные:

CommonName (CN)	Наименование юридического лица	
INN	Индивидуальный номер налогоплательщика юридического лица	
OGRN/OGRNIP	Основной государственный регистрационный номер юридического лица	
Organization (O)	Наименование юридического лица	
Locality (L)	Наименование населённого пункта	Юрид. адрес местонахождения организации
Street Address (STREET)	Название улицы, номер дома, корпуса, помещения	
State (S)	Наименование субъекта РФ	
Country(C)	RU	
SurName(SN)	Фамилия уполномоченного представителя	
GivenName (G)	Имя и отчество уполномоченного представителя	
Title(T)	Наименование должности уполномоченного представителя	
OrganizationUnit (OU)	Наименование подразделения юридического лица	
SNILS	Страховой номер индивидуального лицевого счёта уполномоченного представителя	
E-Mail (E)	Электронный адрес уполномоченного представителя	

Настоящим Я, _____
(паспорт гражданина РФ серия _____ № _____ выдан _____)
даю свое согласие на обработку и использование моих персональных данных, указанных в заявительных документах в течение всего срока деятельности Удостоверяющего центра защищенной сети ОАО «ОЭП». Также признаю, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным. С Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи ознакомлен (-а).

Контактный телефон Уполномоченного представителя 8 ( )

Уполномоченный представитель, данные о котором вносятся в сертификат _____ / _____ /
(подпись) ФИО

_____ _____ / _____ /
(должность руководителя организации) (подпись) ФИО
М.П. « » _____ 201 _ _ года

Приложение № 3
Форма доверенности Пользователя

Доверенность

г. Пенза «___» _____201__ г.

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____,
(должность, фамилия, имя, отчество)
действующего на основании _____,

уполномочивает_____
(фамилия, имя, отчество)
паспорт гражданина РФ _____
(серия и номер паспорта, кем и когда выдан)
действовать от имени _____
(полное наименование организации, включая организационно-правовую форму)

при использовании электронной подписи и осуществлять действия в рамках Регламента Удостоверяющего центра защищенной сети ОАО «ОЭП».

Настоящая доверенность действительна по « ____ » _____ 20__г. без права передоверия.

Подпись уполномоченного представителя подтверждаю. _____ / /
(подпись) (расшифровка подписи)

_____ _____ / /
(должность руководителя организации) (подпись) (расшифровка подписи)

М.П. «____» _____ 201___ года

Приложение № 4

Форма доверенности на получение ключевого документа,
сертификата ключа проверки электронной подписи за
Владельца сертификата и движимого имущества
(материальных ценностей)
в Удостоверяющем центре защищенной сети ОАО «ОЭП»

Доверенность

на получение получение ключевого(-ых) документа(-ов), сертификата (-ов) ключа(-ей) проверки электронной подписи за Владельца(-ев) сертификата и движимого имущества (материальных ценностей) в Удостоверяющем центре защищенной сети ОАО «ОЭП»

г. Пенза «___» _____201__ г.

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____,
(должность, фамилия, имя, отчество)
действующего на основании _____,

уполномочивает_____
(фамилия, имя, отчество)

паспорт гражданина РФ _____
(серия и номер паспорта, кем и когда выдан)

1. предоставить в Удостоверяющий центр защищенной сети ОАО «ОЭП» необходимые документы, определенные Регламентом Удостоверяющего центра защищенной сети ОАО «ОЭП» и получить ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные в Удостоверяющем центре защищенной сети ОАО «ОЭП» для Владельца сертификата

_____
(фамилия, имя, отчество Владельца электронной подписи)

2. получить приобретенное движимое имущество (материальные ценности).

Представитель наделяется правом:

1. расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

2. расписываться в соответствующих документах за получение движимого имущества (материальных ценностей).

Настоящая доверенность действительна по «_____»___201____г. без права передоверия.

Подпись доверенного лица подтверждаю.	_____ (подпись)	/_____/ (расшифровка подписи)
_____ (должность руководителя организации)	_____ (подпись)	/_____/ (расшифровка подписи)

«____» _____ 201_ года

М.П.

Приложение № 5

Форма заявления на аннулирование
сертификата ключа проверки электронной подписи

Заявление на аннулирование
сертификата ключа проверки электронной подписи

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность, фамилия, имя, отчество)
действующего на основании _____

в связи с _____,
(причина отзыва сертификата)

просит аннулировать сертификат ключа проверки электронной подписи своего уполномоченного представителя _____,
(фамилия, имя, отчество)
содержащий следующие данные:

SerialNumber	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Фамилия Имя Отчество уполномоченного представителя

_____ _____ /_____/
(должность руководителя организации) (подпись) (расшифровка подписи)

«____» _____ 201__ года

М.П.

(заполняется сотрудником Удостоверяющего центра)

Данное заявление на аннулирование сертификата ключа проверки электронной подписи зарегистрировано «_____:_____» «_____/_____/_____»
час минута день месяц год

Уполномоченный сотрудник
Удостоверяющего центра ОАО «ОЭП» _____ /_____ /
(подпись) (Ф.И.О.)

М. П.

РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ

- Обеспечьте конфиденциальность ключей электронной подписи.
- Для предотвращения внештатных ситуаций при использовании ключевой информации **ограничьте доступ к компьютеру**, который используется для работы с ключевой информацией и подписания документов электронной подписью. Не доверяйте Ваш компьютер для обслуживания посторонним лицам, исключите бесконтрольный доступ в помещения, в которых размещаются средства электронной подписи.
- Перед первым использованием носителя ключей электронной подписи (ключевого носителя) **измените назначенный по умолчанию PIN-код** (пароль на контейнер). Новый PIN-код должен содержать не менее 8-ми символов случайной цифро-буквенной последовательности.
- **Не передавайте никому личный ключевой носитель и не сообщайте PIN-код к нему** кому бы то ни было. Доступ к ключевому носителю должен быть только у владельца электронной подписи.
- **Не оставляйте личный ключевой носитель и/или PIN-код доступа к нему без присмотра.**
- Обеспечьте безопасное хранение ключей электронной подписи на ключевом носителе в сейфе или запираемом ящике стола.
- **Подсоединяйте ключевой носитель к компьютеру только для подписания электронных документов**, и в обязательном порядке извлекайте его из компьютера сразу после окончания работы. Блокируйте компьютер и извлекайте ключевые носители при уходе с рабочего места.
- **Не извлекайте ключевой носитель во время его работы**, т.к. это может привести к потере данных на нем. Извлечение ключевого носителя должно производиться через «Безопасное извлечение Запоминающего устройства».
- **Старайтесь не наносить повреждений своему ключевому носителю**, не ронять и не ударять, а при извлечении из порта компьютера не менять угол наклона и не раскачивать. Механические повреждения могут привести к поломке ключевого носителя.
- **Не допускается снимать несанкционированные копии с ключевых носителей**, знакомить или передавать ключевые носители лицам, к ним не допущенным, записывать на ключевой носитель с ключами электронной подписи постороннюю информацию.
- **Работайте под учетной записью обычного пользователя** (учетная запись должна быть защищена надежным паролем). Не рекомендуется работа с электронной подписью под учетной записью «Администратор». Отключите стандартную учетную запись «Гость».

- Запретите доступ по сети в вашей организации к каталогам на компьютере, где установлены средства электронной подписи, посторонним лицам.
- Используйте на компьютере только лицензионное программное обеспечение. Своевременно устанавливайте обновления безопасности операционной системы.
- **Обеспечьте непрерывную комплексную защиту компьютера от вирусов,** хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ лицензионным антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления баз данных, с включенной защитой паролем и сетевой защитой, выставленной на максимальный уровень безопасности. Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла. Проводите полную еженедельную проверку компьютера на наличие вирусов.
- В случае утраты личного ключевого носителя и/или PIN-кода доступа к нему для блокировки использования Вашего ключа электронной подписи посторонними лицами **немедленно известите Удостоверяющий центр защищенной сети ОАО «ОЭП» о нарушении конфиденциальности ключа электронной подписи.** Не применяйте ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
- Немедленно обратитесь в Удостоверяющий центр защищенной сети ОАО «ОЭП» с заявлением на аннулирование сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
- Используйте для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
- В организации соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств электронной подписи, назначены владельцы средств электронной подписи и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств; средства электронной подписи и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах.