

Приложение №1 к приказу генерального
директора ООО «ДСЦБИ «МАСКОМ»
№ 54/ДСЦБИ от «08» июня 2017 г.

РЕГЛАМЕНТ
Удостоверяющего центра
департамента информационных технологий
ООО «ДСЦБИ «МАСКОМ»

Оглавление

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	4
1. Общие положения.....	6
1.1. Предмет регулирования регламента	6
1.2. Сведения об УЦ.....	6
1.3. Порядок информирования о предоставлении услуг УЦ	7
1.4. Стоимость услуг УЦ.....	7
2. Перечень функций, реализуемых УЦ	7
3. Права и обязанности	8
3.1. УЦ обязан	8
3.2. Права УЦ.....	9
3.3. Владелец сертификата ключа проверки электронной подписи обязан:	10
3.4. Владелец сертификата ключа проверки электронной подписи вправе:.....	11
3.5. Ответственность сторон	12
4. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг УЦ.....	12
4.1. Процедура создания ключей электронных подписей	12
4.1.1 Способ создания ключей электронной подписи.....	12
4.1.2. Порядок осуществления плановой смены ключей электронной подписи УЦ	12
4.1.3. Порядок осуществления внеплановой смены ключей электронной подписи УЦ при их компрометации.....	13
4.1.4. Порядок осуществления УЦ смены ключа электронной подписи владельца сертификата	13
4.2. Процедура создания и выдачи сертификатов	13
4.2.1. Порядок подачи заявления на создание и выдачу сертификатов и требования к такому заявлению	13
4.2.2. Порядок установления личности заявителя	14
4.2.3. Перечень документов, запрашиваемых у заявителя для изготовления (создания) и выдачи сертификата.....	15
4.2.4. Изготовление (создание) сертификата.....	16
4.2.5. Выдача и отказ в выдаче сертификата ключа проверки электронной подписи	16
4.2.6. Срок создания и выдачи ключа электронной подписи и ключа проверки электронной подписи владельцу.....	16
4.3. Аннулирование и прекращение действия сертификата	16
4.3.1. Условия (основания) аннулирования или прекращения действия сертификата	16
4.4. Порядок ведения реестра сертификатов.....	17

4.4.1. Информация о реестре сертификатов	17
4.4.2. Обновление реестра сертификатов	18
4.4.3. Контроль доступа к реестру сертификатов ключей проверки электронных подписей ...	18
4.5. Подтверждение действительности электронной подписи, использованной для подписания электронных документов (разбор конфликтной ситуации).....	18
5. Порядок исполнения обязанностей УЦ	19
5.1. Использование ключей электронной подписи и сертификатов ключей проверки электронных подписей	19
5.1.1. Использование ключа проверки электронной подписи и сертификата ключа проверки электронной подписи владельцем.....	19
5.1.2. Обновление сертификата ключа проверки электронной подписи.....	20
5.1.3. Изменение сведений, указанных в сертификате ключа проверки электронной подписи	20
5.1.4. Резервное копирование ключа электронной подписи.....	20
5.1.5. Архивирование ключа электронной подписи	20
5.1.6. Способы активации ключа электронной подписи	20
5.1.7. Способы деактивации ключа электронной подписи	21
5.1.8. Способы уничтожения ключа электронной подписи	21
5.1.9. Сроки действия сертификатов и ключей	21
5.2. Политика конфиденциальности	21
5.2.1. Типы конфиденциальной информации.....	21
5.2.2. Типы информации, не являющейся конфиденциальной.....	21
5.2.3. Исключительные полномочия официальных лиц	22
5.2.4. Обработка персональных данных в УЦ.....	22
5.3. Регистрация квалифицированного сертификата владельца в ЕСИА.....	22
Приложение №1	23
Приложение №2	24
Приложение №3	25
Приложение №4	26
Приложение №5	27
Приложение №6	28
Приложение №7	29
Приложение №8	30
Приложение №9	31
Приложение №10	32

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор Удостоверяющего центра - сотрудник Удостоверяющего центра департамента информационных технологий (далее - УЦ), уполномоченный производить действия, связанные с инсталляцией, конфигурированием и поддержкой УЦ, созданием новых членов администраторов, проведением аудита работоспособности и безопасности системы, архивированием, резервным копированием и восстановлением информации после сбоев, изданием и отзывом сертификатов, просмотром и поддержкой журналов аудита.

Владелец сертификата ключа проверки электронной подписи (далее также – владелец сертификата) – лицо, которому в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», выдан (далее также - вручён) сертификат ключа проверки электронной подписи.

Вручение сертификата ключа проверки электронной подписи - передача уполномоченным лицом УЦ изготовленного от имени УЦ сертификата ключа проверки электронной подписи его владельцу.

Заявитель – лицо, обратившееся в установленном настоящим регламентом порядке в УЦ (в частности, путём подачи соответствующего заявления) с целью получения средств электронной подписи.

Компрометация ключа – утрата доверия к тому, что используемые ключи электронной подписи или ключи проверки электронной подписи обеспечивают безопасность информации, защищаемой с их использованием.

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

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

Регламент УЦ – настоящий документ, отражающий основные права и обязанности УЦ и владельцев сертификатов, порядок взаимодействия указанных лиц, а также их взаимодействия с заинтересованными лицами, порядок работы УЦ в соответствии с его функциями, а также основные организационно-технические мероприятия, необходимые для функционирования УЦ в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Регистрация владельца сертификата ключа проверки электронной подписи – внесение информации о владельце сертификата ключа проверки электронной подписи в реестр УЦ, применяемое в отношении физических лиц, обращающихся к услугам УЦ в части изготовления сертификатов ключей проверки электронной подписей и изготовления ключей электронной подписи, ключей проверки электронных подписей с записью их на защищённый носитель.

Сертификат ключа проверки электронной подписи (далее также – сертификат) – электронный документ или документ на бумажном носителе, выданный УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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.

Список отозванных сертификатов – электронный документ с электронной подписью уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов, которые на определённый момент времени были отозваны (аннулированы).

Смена ключей – процедура выдачи нового сертификата ключа проверки электронной подписи, подразумевающая изготовление нового ключа электронной подписи и ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) департамента информационных технологий Общества с ограниченной ответственностью «Дальневосточный специализированный центр безопасности информации «МАСКОМ», осуществляющий функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи» в соответствии с требованиями, предъявляемым Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Приказом ФСБ России от 27.12.2011 № 795 к удостоверяющим центрам.

Уполномоченное лицо УЦ – физическое лицо, из числа штатных сотрудников УЦ, наделённый полномочиями по приёму документов, генерации ключей и выдаче ключей проверки электронных подписей, а также по заверению копий сертификатов ключей проверки электронных подписей в бумажном виде, заверению сертификатов ключей проверки электронных подписей в электронном виде и списков отозванных сертификатов, а также иными полномочиями, согласно настоящего регламента и действующего законодательства Российской Федерации.

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

1. Общие положения

1.1. Предмет регулирования регламента

Настоящий регламент является документом, который отражает основные права и обязанности УЦ и владельцев сертификатов, порядок взаимодействия указанных лиц, а также их взаимодействия с заинтересованными лицами, порядок работы УЦ в соответствии с его функциями, а также основные организационно-технические мероприятия, необходимые для функционирования УЦ.

Настоящий регламент распространяется в форме электронного документа и размещён для свободного доступа по адресу: <http://uc-mascom.ru/files/ca-documents/ca-dscbi-reglament.pdf>

Внесение изменений (дополнений) в регламент, включая приложение к нему, производится УЦ в одностороннем порядке. Уведомление третьих лиц о внесении изменений (дополнений) в регламент осуществляется УЦ путём обязательного размещения очередной редакции настоящего регламента на сайте УЦ по адресу: <http://uc-mascom.ru/files/ca-documents/ca-dscbi-reglament.pdf>.

Присоединение к настоящему регламенту (принятие его условий) осуществляется путём подписания лицом и предоставления в УЦ заявления на изготовление (создание) сертификата владельцу (далее – заявитель) по форме, установленной Приложением № 1 и 2 к настоящему регламенту.

С момента получения заявления, лицо подавшее такое заявление, считается присоединившимся к настоящему регламенту (принявшим его условия). С момента присоединения к настоящему регламенту, лицо соглашается с его требованиями регламента и приложениями к нему и обязуется соблюдать все их положения (статья 428 Гражданского кодекса Российской Федерации).

Лицо, присоединившись к настоящему регламенту, самостоятельно, путём самостоятельного ознакомления с текстом регламента на сайте УЦ отслеживает изменения (дополнения), вносимые в настоящий регламент в виде его новой редакции.

1.2. Сведения об УЦ

Деятельность УЦ направлена на обеспечение условий для внедрения технологий электронной подписи и надлежащего использования электронной подписи в информационных системах.

Основные функции УЦ регламентируются Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». УЦ предназначен для обработки информации, не содержащей сведений составляющих государственную тайну.

УЦ является структурным подразделением Общества с ограниченной ответственностью «Дальневосточный специализированный центр безопасности информации «МАСКОМ» (ООО «ДСЦБИ «МАСКОМ», ОГРН 1152724009184, адрес места нахождения: 680009, г. Хабаровск, ул. Хабаровская, д. 15) и расположен по адресу: 680038, г. Хабаровск, ул. Яшина, д. 40.

УЦ находится в прямом подчинении начальника УЦ.

В своей деятельности УЦ руководствуется законодательством Российской Федерации, в части касающейся электронной подписи, и настоящим регламентом.

Деятельность УЦ осуществляется на основании лицензии Управления Федеральной службы безопасности Российской Федерации (ФСБ России) по Хабаровскому краю №ХК/1753 от 09.07.2014 на осуществление разработки, производства, распространения

шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения нужд юридического лица или индивидуального предпринимателя).

Режим работы УЦ: в рабочие дни – с 09:00 до 18:00 по хабаровскому времени (перерыв на обед с 13:00 до 14:00); выходные дни – суббота, воскресенье.

1.3. Порядок информирования о предоставлении услуг УЦ

Информирование заинтересованных лиц о предоставляемых услугах УЦ осуществляется:

- в круглосуточном режиме на сайте УЦ по адресу: <http://uc-mascom.ru/dscbi>;
- в часы работы УЦ по многоканальному телефонному номеру в г. Хабаровске: 8 (4212) 45-46-34, а также по электронной почте: uc@mascom-dv.ru.

Для получения информации по вопросам предоставления услуг УЦ необходимо:

- оставить заявку в часы работы УЦ по вышеуказанным телефонным номерам в г. Хабаровске, а также по электронной почте.
- посетить офис обслуживания по адресу: 680038, г. Хабаровск, ул. Яшина, 40.

1.4. Стоимость услуг УЦ

УЦ осуществляет свою деятельность на возмездной основе, кроме случаев, установленных настоящим регламентом или законодательством Российской Федерации.

Стоимость услуг УЦ по настоящему регламенту устанавливается в соответствии с прейскурантом цен на услуги размещённого на сайте УЦ.

Информирование заинтересованных лиц о стоимости услуг УЦ осуществляется путём размещения прейскуранта цен на сайте УЦ.

Оплата услуг УЦ осуществляется авансом, путём внесения денежных средств на расчётный счёт ООО «ДСЦБИ «МАСКОМ» в течение 3 рабочих дней с момента подписания заявителем и УЦ договора на предоставление услуг/.

2. Перечень функций, реализуемых УЦ

- создание и выдача сертификатов при условии установления личности заявителя либо полномочия лица, выступающего от его имени при обращении за получением данного сертификата;
- осуществление (в соответствии с правилами подтверждения владения ключом электронной подписи) подтверждения владения получателем сертификата ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата;
- установление сроков действия сертификатов;
- аннулирование выданных УЦ сертификатов;

- выдача средств электронной подписи, содержащих ключ электронной подписи и ключ проверки электронной подписи или обеспечивающих возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведение реестра выданных и аннулированных УЦ сертификатов ключей проверки электронных подписей, в том числе включающего в себя информацию, содержащуюся в выданных УЦ сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования;
- создание ключей электронных подписей и ключей проверки электронных подписей по обращению заявителей;
- проверка уникальности ключей проверки электронных подписей в реестре сертификатов;
- осуществление проверки электронных подписей по обращению их владельцев;
- реализация системы оповещения владельцев сертификатов с использованием электронных почтовых сообщений;
- ведение реестра зарегистрированных владельцев сертификатов;
- ведение реестра запросов на сертификаты ключей проверки электронной подписи и сертификаты ключей шифрования в электронном виде;
- ведение реестра запросов и заявлений на аннулирование (отзыв) действия сертификатов ключей проверки электронных подписей или сертификатов ключей шифрования в электронном виде;
- хранение конфиденциальной информации в форме, позволяющей проверить ее целостность и достоверность в течение всего срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации.
- осуществление иных функции, необходимых для осуществления деятельности, указанной в п. 1.2. настоящего регламента.

3. Права и обязанности

3.1. УЦ обязан

- информировать в письменной форме заявителей об условиях и 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;
- вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;
- создавать по обращению заявителей ключи электронных подписей и ключи проверки электронных подписей;
- создавать сертификаты ключей проверки электронных подписей;
- выдавать сертификаты заявителям, обратившимся за их получением;
- устанавливать сроки действия сертификатов ключей проверки электронных подписей;
- прекращать действие или аннулировать выданные сертификаты ключей проверки электронных подписей;
- выдавать по обращению заявителей средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи;

- обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечивать круглосуточную доступность реестра сертификатов в информационно-коммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания;
- обеспечивать конфиденциальность созданных УЦ ключей электронных подписей;
- в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» направлять в единую систему идентификации и аутентификации сведения о лице, получившем сертификат ключа проверки электронной подписи (далее также – квалифицированный сертификат), в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра);
- по желанию владельца, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию указанного лица в единой системе идентификации и аутентификации;
- отказать заявителю в создании сертификата в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата;
- отказать заявителю в создании сертификата в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата;
- строго соблюдать срок действия ключей электронной подписи УЦ, используемых для подписания создаваемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие.

3.2. Права УЦ

В рамках исполнения возложенных на него функций, УЦ вправе:

- запрашивать у заявителя документы для подтверждения любой содержащейся в заявлении на создание и выдачу сертификата информации;
- с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем;
- запрашивать и получать из государственных информационных ресурсов:
 - выписку из единого государственного реестра юридических лиц в отношении заявителя – юридического лица;
 - выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя – индивидуального предпринимателя;
 - выписку из Единого государственного реестра налогоплательщиков в отношении заявителя – иностранной организации.

- запросить у заявителя дополнительные, подтверждающие достоверность представленных им сведений документы в случае наличия противоречий между сведениями, представленными заявителем и сведениями, полученными УЦ, а также в случае, если такие сведения необходимы для формулирования и подтверждения информации в сертификате ключа проверки электронной подписи;

- не принимать от заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации;

- отказать заявителю в выдаче сертификата в случае невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим регламентом;

- отказать владельцу сертификата в прекращении действия сертификата в случае, если сертификат уже аннулирован или прекратил своё действие по другим основаниям;

- отказать в изготовлении сертификата ключа проверки электронной подписи владельцам сертификатов, подавшим заявление на изготовление сертификата ключа проверки электронной подписи, с указанием причин отказа;

- аннулировать или прекратить действие по заявлению владельца сертификата действие сертификата ключа проверки электронной подписи, выданного в соответствии настоящим регламентом;

- без заявления владельца сертификата прекратить действие сертификата в случае наличия у УЦ достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата, а также невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи, а также в случае появления у УЦ достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включённой в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

- назначать и согласовывать с владельцем сертификата ключа проверки электронной подписи дату явки последнего в УЦ для выполнения процедур, предусмотренных настоящим регламентом;

- назначать дату проведения работ по установке средств ЭП на рабочем месте владельца сертификата;

- запрашивать информацию в случаях проведения экспертизы подлинности ЭП на электронных документах, при разборе конфликтных ситуаций, при осуществлении УЦ своей деятельности.

3.3. Владелец сертификата ключа проверки электронной подписи обязан:

- обращаться в УЦ для изготовления, создания и обновления ключей электронной подписи в соответствии с настоящим регламентом;

- предоставить для заключения договора на предоставление услуг УЦ комплект документов и гарантировать достоверность сведений, указываемых в заявлении на изготовление сертификата, и соответствие сведений учредительным документам владельца, а также правоспособность и (или) дееспособность уполномоченного представителя владельца;

- при наступлении случаев, ограничивающих правоспособность или дееспособность владельца, незамедлительно уведомить об этом УЦ и произвести действия по аннулированию сертификата согласно регламента УЦ;
- использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с законодательством Российской Федерации.
- пройти соответствующую подготовку в УЦ, получить «Заключение о проведении обучения владельцу сертификата при работе с СКЗИ и ЭП» и «руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи»;
- соблюдать требования «руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи»;
- использовать электронную подпись в соответствии с ограничениями, содержащимися в таком сертификате (если такие ограничения установлены);
- обеспечивать конфиденциальность ключа электронной подписи, в частности не допускать использование принадлежащих владельцу сертификата ключей электронных подписей без его согласия;
- не использовать ключ электронной подписи и немедленно обратиться в УЦ для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- уведомлять УЦ 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;
- в случае прекращения трудовых отношений (по любой причине) сотрудника владельца сертификата, на имя которого УЦ выдан такой сертификат, немедленно обратиться в УЦ с заявлением на аннулирование сертификата;
- при работе со средствами электронной подписи использовать только лицензионное антивирусное программное обеспечение с регулярно обновляемыми базами;
- в работе со средствами электронной подписи руководствоваться эксплуатационной и технической документацией к таким средствам, а также требованиями законодательства Российской Федерации;
- самостоятельно нести ответственность, установленную действующим законодательством Российской Федерации, перед третьими лицами, а также риски убытков из-за несоблюдения требований настоящего регламента.

3.4. Владелец сертификата ключа проверки электронной подписи вправе:

- создавать, передавать, обрабатывать, хранить электронные документы в рамках сведений, содержащихся в сертификате;
- обращаться в УЦ за проведением экспертизы подлинности электронной подписи в электронном документе;
- получать в УЦ консультации по вопросам работы с электронной подписью и средствами криптографической защиты информации;

- осуществлять иные права, установленные инструкциями и другими нормативными документами.

3.5. Ответственность сторон

УЦ несёт ответственность, установленную действующим законодательством Российской Федерации.

УЦ не несёт ответственность за ущерб, понесённый владельцем сертификата в результате утраты доверия к такому сертификату, а также за последствия компрометации владельца ключа электронной подписи, если УЦ выполнил все требования действующего законодательства и договора на предоставление услуг УЦ.

УЦ не несёт ответственность за неготовность владельца сертификата к использованию ключа электронной подписи, обусловленной неисполнением или ненадлежащим исполнением обязанностей владельца, установленных настоящим регламентом.

УЦ не несёт ответственность за незаконные действия третьих лиц, в результате которых ключ электронной подписи владельца сертификата становится доступным третьим лицам (в том числе, в результате хакерских атак). Ответственность перед владельцем сертификата за весь причинённый ему вред в указанном случае несут непосредственно третьи лица, осуществившие данные незаконные действия (хакерские атаки).

УЦ не несёт ответственности за неисполнение обязательств перед владельцем сертификата, обусловленное неудовлетворительным качеством каналов связи, абонентских линий, телекоммуникационного оборудования владельца сертификата, а также сбои программного обеспечения, установленного на рабочем месте владельца сертификата.

За предоставление недостоверных сведений заявители несут ответственность в соответствии с законодательством Российской Федерации.

4. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг УЦ

4.1. Процедура создания ключей электронных подписей

4.1.1 Способ создания ключей электронной подписи

Администратор УЦ в соответствии со сведениями, указанными в заявлении, на специализированном рабочем месте УЦ создаёт ключ электронной подписи как в присутствии заявителя, так и без такового.

При реализации способа создания ключа электронной подписи на специализированном рабочем месте УЦ используется автоматизированное рабочее место. Ключ электронной подписи, созданный таким образом, записывается УЦ на ключевой носитель, который выдаётся заявителю либо доверенному лицу заявителя по окончании процедуры выдачи сертификата.

При создании ключей электронной подписи администратор УЦ должен выполнять требования по обеспечению безопасности информации, соответствующие законодательству Российской Федерации по технической защите конфиденциальной информации.

4.1.2. Порядок осуществления плановой смены ключей электронной подписи УЦ

В соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» уполномоченный федеральный орган исполнительной власти осуществляет плановую смену и выдачу квалифицированного сертификата для уполномоченного лица УЦ,

создаваемого с использованием средств головного удостоверяющего центра такого федерального органа.

Срок действия сертификата уполномоченного лица УЦ не превышает 10 (десять) лет.

Заблаговременно до окончания срока действия квалифицированного сертификата уполномоченного лица УЦ, администратор УЦ производит формирование нового запроса на квалифицированный сертификат уполномоченного лица УЦ и направляет его в уполномоченный федеральный орган исполнительной власти.

Новый сертификат записывается на электронный носитель и передаётся начальнику УЦ вместе с бланком сертификата.

Информирование владельцев сертификатов об осуществлении смены квалифицированного сертификата уполномоченного лица УЦ осуществляется с помощью размещения нового квалифицированного сертификата на сайте УЦ по адресу: <http://uc-mascom.ru/files/korn-cp-dscbi.cer>.

Все владельцы сертификатов ключей проверки электронных подписей обязаны получить новый квалифицированный корневой сертификат и добавить его в справочники сертификатов без удаления действующего корневого сертификата.

4.1.3. Порядок осуществления внеплановой смены ключей электронной подписи УЦ при их компрометации

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа электронной подписи уполномоченного лица УЦ.

Процедура внеплановой смены ключей уполномоченного лица УЦ выполняется в порядке, определённом процедурой плановой смены ключей, установленной пп.4.1.2. настоящего регламента. При этом, одновременно со сменой такого ключа электронной подписи прекращается действие всех сертификатов владельцев сертификатов, подписанных этим ключом электронной подписи, с занесением сведений об этих сертификатах в реестр сертификатов.

В случае выполнения внеплановой смены ключа электронной подписи УЦ безвозмездно создаёт сертификаты для всех владельцев сертификатов, чьи сертификаты прекращают действие в связи с внеплановой заменой.

4.1.4. Порядок осуществления УЦ смены ключа электронной подписи владельца сертификата

Процедура осуществления смены ключа электронной подписи владельца сертификата полностью аналогична процедуре подачи создания и выдачи сертификатов, установленной п.4.2. настоящего регламента

4.2. Процедура создания и выдачи сертификатов

4.2.1. Порядок подачи заявления на создание и выдачу сертификатов и требования к такому заявлению

Заявление на создание и выдачу сертификатов осуществляется на основании заявления лица по форме, установленной приложением № 1 и 2 к настоящему регламенту.

Указанное в настоящем подпункте заявление может быть подано (оформлено) как на бумажном носителе, так и в форме электронного документа. Одновременно с заявлением

заявителем предоставляются предусмотренные настоящим регламентом документы, необходимые для установления его личности и выпуска ему сертификата.

Заявление, поданное от физического лица (приложение № 2 к настоящему регламенту), должно обязательно содержать следующие сведения:

- фамилию, имя и отчество (при наличии);
- паспортные данные заявителя;
- страховой номер индивидуального лицевого счета (СНИЛС);
- адрес электронной почты;
- контактные телефоны.

Заявление, поданное от имени юридического лица (приложение № 1 к настоящему регламенту), должно обязательно содержать следующие сведения:

- информацию, указанную в абзаце третьем настоящего подпункта, о физическом лице, на имя которого будет выдан сертификат;
- полное и сокращённое наименования юридического лица, указанные в его учредительных документах;
- должность и подразделение (при наличии) лица, представляющего юридическое лицо;
- данные доверенности (или других документов, подтверждающих полномочия действовать от имени юридического лица);
- почтовый и юридический адрес (адрес места нахождения) юридического лица;
- ИНН;
- КПП;
- ОГРН;
- банковские реквизиты;
- субъект Федерации, в котором зарегистрировано юридическое лицо.

При подачи заявления заявитель указывает на ограничения использования сертификата (если такие ограничения им устанавливаются).

Заявление подаётся заявителем лично или через представителя, уполномоченного на это нотариальной доверенностью (приложение № 7 - 10 к настоящему регламенту) или учредительным документом юридического лица, в УЦ.

При подаче заявления на выпуск сертификата, содержащего персональные данные, заявитель письменно выражает своё согласие на обработку его персональных данных и признает, что персональные данные, вносимые в сертификаты, владельцем которых он является, относятся к общедоступным персональным данным.

4.2.2. Порядок установления личности заявителя

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, УЦ может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации.

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учётом требований п. 4.2.3. настоящего регламента.

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

4.2.3. Перечень документов, запрашиваемых у заявителя для изготовления (создания) и выдачи сертификата

Одновременно с подачей заявления в соответствии с пп. 4.2.1. настоящего регламента, заявитель предоставляет в УЦ следующие документы, подтверждающие изложенную в таком заявлении информацию:

- 2-й и 3-й страниц общегражданского паспорта, а также страницы с указанием последнего места регистрации лица;
- страховое свидетельство обязательного пенсионного страхования (СНИЛС) лица;
- доверенность, подтверждающую полномочия владельца сертификата (приложение № 10 к настоящему регламенту);
- паспорт гражданина Российской Федерации и нотариальная доверенность на представителя юридического лица, уполномоченного на предоставление документов для изготовления сертификата и/или получение изготовленного сертификата (приложение № 7 и 8 к настоящему регламенту).

Заявитель вправе по собственной инициативе представить копии (заверенные нотариусом, либо УЦ, если заявителем будет предъявлен оригинал) документов, содержащих сведения, указанные заявителем в заявлении, в частности:

- свидетельство о государственной регистрации юридического лица;
- свидетельство о постановке на учёт юридического лица в налоговом органе;
- свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя;
- свидетельство о постановке на учёт в налоговом органе физического лица по месту жительства в Российской Федерации;
- решение (протокол) о назначении лица, уполномоченного действовать от имени юридического лица без доверенности;

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

Если от имени заявителя – физического лица действует другое физическое лицо на основании доверенности (приложение № 8 к настоящему регламенту), такая доверенность должна быть удостоверена нотариально.

УЦ оставляет за собой право осуществлять проверку сведений, указанных в заявлении на выдачу сертификата ключа проверки электронной подписи.

УЦ вправе требовать от заявителя представления дополнительных документов:

- подтверждающих сведения, указанные в заявлении, в случае, если выявлены противоречия между сведениями (документами) предоставленными заявителем и сведениями, полученными УЦ в установленном законодательством порядке;
- в случае установления операторами государственных, муниципальных информационных систем, а также иных информационных систем дополнительных требований к созданию пространства доверия сертификатов владельцев, изготавливаемых УЦ.

4.2.4. Изготовление (создание) сертификата

Сертификат ключа проверки электронной подписи изготавливается администратором УЦ в соответствии со сведениями, указанными в заявлении, на специализированном рабочем месте.

В качестве ключевых носителей (электронных идентификаторов) используются только носители, указанные в эксплуатационной документации средства, с помощью которых производится изготовление ключей.

Уведомление заявителя о факте изготовления сертификата ключа проверки электронной подписи осуществляется по телефону или адресу электронной почты, указанному в сертификате.

4.2.5. Выдача и отказ в выдаче сертификата ключа проверки электронной подписи

УЦ выдаёт две копии сертификата ключа проверки электронной подписи в форме документов на бумажном носителе, в случае успешного прохождения заявителем процедур и совершения действия, указанных в пп. 4.2.1. – 4.2.3. настоящего регламента.

УЦ вправе отказать заявителю в выдаче сертификата ключа подписи в случае невозможности подтверждения сведений, указанных в заявлении или выявления противоречий между сведениями (документами) предоставленными заявителем и сведениями, полученными УЦ в установленном законодательством порядке (если такие противоречия не были разрешены в установленном настоящим регламентом порядке).

Ключевой носитель (электронный идентификатор) с ключом электронной подписи и ключом проверки электронной подписи передаётся владельцу или его законному представителю (приложением № 7 и 8 к настоящему регламенту) после установки в него сертификата ключа проверки электронной подписи.

4.2.6. Срок создания и выдачи ключа электронной подписи и ключа проверки электронной подписи владельцу

Срок создания и выдачи сертификата не превышает 5 (пять) календарных дней с момента получения УЦ соответствующего заявления и необходимых документов.

4.3. Аннулирование и прекращение действия сертификата

4.3.1. Условия (основания) аннулирования или прекращения действия сертификата

УЦ может аннулировать сертификат ключа проверки электронной подписи и осуществить публикацию его в списке отозванных сертификатов в следующих случаях:

- 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;
- получение от владельца сертификата ключа проверки электронной подписи заявления об аннулировании сертификата, подаваемого в форме документа на бумажном носителе или в

форме электронного документа в соответствии с приложением № 3 и 4 к настоящему регламенту.

Указанные в настоящем подпункте заявления может подавать только его владелец (в случае, если в сертификате указаны сведения о юридическом лице, от имени которого действует его владелец – уполномоченное лицо юридического лица). Подтверждение полномочий лица, подавшего заявление на аннулирование (прекращение действия) сертификата ключа проверки электронной подписи осуществляется в порядке, установленном для подачи заявлений на выдачу такого сертификата.

Заявление на аннулирование (прекращение действия) сертификата ключа проверки электронной подписи следует подавать в течение минимально возможного времени после появления такой необходимости (например, в случае компрометации ключа электронной подписи).

Срок обработки заявления на аннулирование (прекращение действия) сертификата ключа проверки электронной подписи составляет не более 30 минут с момента принятия такого заявления.

Владелец сертификата ключа проверки электронной подписи должен проверять факт аннулирования (прекращения действия) сертификата, на достоверность которого он полагается. Проверка факта отзыва может осуществляться с использованием списков отозванных сертификатов или сервиса онлайн-проверки статуса сертификата, сведения о порядке доступа к которым указаны в каждом выданном УЦ сертификате ключа проверки электронной подписи и настоящем регламенте.

Списки отозванных сертификатов публикуются не реже одного раза в сутки. Сертификаты с истекшим сроком действия, удаляются из списков отозванных сертификатов.

Информация об аннулировании (прекращении действия) сертификата ключа проверки электронной подписи публикуется, в течение 20 минут после отзыва.

4.4. Порядок ведения реестра сертификатов

4.4.1. Информация о реестре сертификатов

Реестр сертификатов ключей проверки электронных подписей ведётся в обязательном порядке в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Реестр сертификатов ключей проверки электронных подписей функционирует на оборудовании УЦ в здании, расположенном по адресу: г. Хабаровск, ул. Яшина, 40.

Реестр сертификатов ключей проверки электронных подписей ведётся по протоколу NTTPS. Адрес такого реестра в сети: <https://pki.mascom-dv.ru:1311/CertificateRegistry15/>.

Реестр сертификатов служит для выполнения следующих функций:

- хранения выданных (действующих и недействующих) сертификатов ключей проверки электронных подписей;
- хранения списка аннулированных сертификатов и сертификатов, действие которых прекращено (далее также – список отозванных сертификатов);
- хранения сертификатов ключей УЦ;
- обеспечения доступа всех владельцев сертификатов к хранимой в таком реестре информации.

УЦ осуществляет непосредственное управление реестром сертификатов ключей проверки электронных подписей, обеспечивая требуемый уровень доступности и актуальности, контролирование доступа, а также целостность информации.

4.4.2. Обновление реестра сертификатов

Включение нового сертификата ключа проверки электронной подписи в Реестр сертификатов должно производиться в течение рабочего дня формирования сертификата ключа проверки электронной подписи, но не позднее даты начала его действия, указанной в сертификате и не позднее формальной выдачи сертификата владельцу.

Обновление списка отозванных сертификатов производится не менее 1 раза в сутки. Обновление списков отозванных сертификатов может быть проведено внепланово если произошли следующие события:

- УЦ стало достоверно известно о прекращении действия документа, на основании которого был выдан данный сертификат ключа проверки электронной подписи;
- поступления заявления об аннулировании сертификата ключа проверки электронной подписи от владельца или от другого уполномоченного лица.

При внеплановом обновлении списков отозванных сертификатов все владельцы УЦ должны иметь возможность узнать о данном факте.

4.4.3. Контроль доступа к реестру сертификатов ключей проверки электронных подписей

Владельцы сертификатов УЦ должны иметь доступ к реестру сертификатов в любое время.

Реестр сертификатов ключей проверки электронных подписей УЦ имеет защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий владельцев сертификатов за счёт фильтрации нежелательного трафика межсетевым экраном, входящим в состав комплекса программно-технических средств УЦ, на основании predetermined правил фильтрации.

Любые модификации реестра сертификатов производятся только администратором УЦ.

Физическое размещение реестра сертификатов соответствует требованиям информационной безопасности.

4.5. Подтверждение действительности электронной подписи, использованной для подписания электронных документов (разбор конфликтной ситуации)

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным заявителем. Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников УЦ.

Разбор конфликтной ситуации проводится на автоматизированном рабочем месте разбора конфликтных ситуаций (далее - АРМ РКС) для электронного документа, авторство или содержание которого оспаривается.

Для проведения разбора конфликтной ситуации при проверке ЭП документа, владельцу необходимо предоставить:

- заявление на проведение подтверждения действительности электронной подписи в электронном документе (приложение № 5 и 6 к настоящему регламенту);

- заверенный УЦ сертификат ключа проверки электронной подписи владельца, подписавшего документ, подлинность или авторство которого оспаривается;
- ключевой носитель, содержащий сертификат ключа проверки электронной подписи, ключ электронной подписи и ключ проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе;
- файл, содержащий текст документа и электронную подпись его автора, в отношении которого возникает конфликтная ситуация.

При проверке ЭП документа, выполняется проверка действительности всех сертификатов, включённых в цепочку проверки для данного сертификата до сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром, а также отсутствия сертификата в списке отозванных сертификатов (CRL), авторство подписи под документом считается установленным.

Несовпадение даты формирования документа и сроков действия сертификата и/или сроков действия ключа ЭП не влияют на определение авторства документа. На их основе делается вывод о несоблюдении владельцем сертификата требований настоящего регламента в части сроков действия ключей, сертификатов или некорректного использования сертификата в прикладном программном обеспечении.

Протокол проверки ЭП, формируемый в АРМ РКС выдаётся владельцу сертификата и является основным документом работы комиссии, который должен быть подписан всеми членами комиссии.

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению владельцу сертификата протокола по выполненной проверке составляет три рабочих дня с момента поступления заявления в УЦ. Услуга по подтверждению подлинности электронной подписи в электронном документе осуществляется на безвозмездной основе.

5. Порядок исполнения обязанностей УЦ

5.1. Использование ключей электронной подписи и сертификатов ключей проверки электронных подписей

5.1.1. Использование ключа проверки электронной подписи и сертификата ключа проверки электронной подписи владельцем

Использование владельцем ключа электронной подписи и сертификата ключа проверки электронной подписи допускается только после признания сертификата. Владелец сертификата должен использовать сертификат строго в соответствии с настоящим регламентом и сведениями, указанными в этом сертификате.

Получение дополнительных сведений и гарантий, помимо указанных в сертификате ключа проверки электронной подписи, осуществляется владельцем сертификата самостоятельно в случае необходимости.

До принятия решения о доверии к сертификату и/или электронной подписи, владелец сертификата должен проверить:

- допустимость использования сертификата в соответствии со сведениями об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение;
- сведения о статусе сертификата ключа проверки электронной подписи;

- в тех случаях, когда действие сертификата прекращено (сертификат аннулирован), или информацию о его статусе получить невозможно, владелец сертификата должен самостоятельно принять решение об использовании такого сертификата; в этом случае все риски, связанные с доверием к такому сертификату несёт владелец сертификата.

5.1.2. Обновление сертификата ключа проверки электронной подписи

Процедура выдачи сертификата ключа проверки электронной подписи без изменения ключа электронной подписи и ключа проверки электронной подписи, а также сведений, указанных в сертификате, не производится.

Для непрерывного использования услуг УЦ, владелец сертификата ключа проверки электронной подписи должен производить ежегодную плановую смену ключей электронной подписи и получать новый сертификат ключа проверки электронной подписи до момента окончания срока действия актуального сертификата. Ключи электронных подписей и сертификаты ключей проверки электронных подписей выдаются их владельцам сроком на 1 (один) год или иной срок, не превышающий максимальный срок действия ключей электронных подписей и сертификатов ключей проверки электронных подписей, установленный используемым средством электронной подписи (средством криптографической защиты информации). Конкретный срок действия ключей электронных подписей и сертификатов ключей проверки электронных подписей устанавливается УЦ при их изготовлении и доводится до владельцев сертификатов в момент получения или средств электронной подписи.

Не позднее, чем за две недели до истечения срока действия сертификата ключа проверки электронной подписи, его владелец должен подать заявление на выдачу нового ключа электронной подписи.

5.1.3. Изменение сведений, указанных в сертификате ключа проверки электронной подписи

Процедура подачи заявления и выдачи сертификата ключа проверки электронной подписи при изменении сведений, указанных в сертификате, полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки.

5.1.4. Резервное копирование ключа электронной подписи

Резервное копирование ключа электронной подписи осуществляется владельцем самостоятельно. К резервной копии применяются те же требования, что и к оригиналу.

5.1.5. Архивирование ключа электронной подписи

УЦ не депонирует и не архивирует ключи электронной подписи владельцев.

Ключи электронных подписей с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией средств криптографической защиты информации.

5.1.6. Способы активации ключа электронной подписи

Все владельцы сертификатов ключей проверки электронных подписей обязаны хранить и защищать свои ключи электронных подписей в соответствии с требованиями эксплуатационной документации средства криптографической защиты информации и действующим законодательством.

Активация ключа электронной подписи происходит при подключении ключевого носителя к персональному компьютеру с установленным необходимым для работы программным обеспечением, после ввода PIN-кода.

Данные активации (PIN-код), предназначены для защиты ключевых носителей. Ключи электронной подписи на ключевом носителе защищаются паролем (PIN-кодом). Пароль (PIN-код) формирует лицо, выполняющее процедуру создания ключей, в соответствии с требованиями на используемое средство электронной подписи.

Если процедуру создания ключей владельцу сертификата выполняет администратор УЦ, то он должен сообщить сформированный пароль (PIN-код) владельцу сертификата в момент получения такого ключа владельцем.

PIN-код должен быть известен только владельцу сертификата. Ответственность за конфиденциальность сохранения пароля PIN-кода возлагается только на владельца сертификата.

5.1.7. Способы деактивации ключа электронной подписи

Ключ электронной подписи деактивируется средством криптографической защиты информации автоматически после выполнения связанных с его использованием операций или после физического отключения ключевого носителя от персонального компьютера.

5.1.8. Способы уничтожения ключа электронной подписи

Уничтожение ключа электронной подписи производится в соответствии с эксплуатационной документацией средства криптографической защиты информации.

5.1.9. Сроки действия сертификатов и ключей

Срок действия сертификатов и ключей не превышает срок, указанный в документе на сертифицированное средство электронной подписи.

5.2. Политика конфиденциальности

5.2.1. Типы конфиденциальной информации

Ключ электронной подписи владельца сертификата ключа проверки электронной подписи является конфиденциальной информацией.

Персональная информация владельцев сертификатов, содержащаяся в УЦ, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи и списка отозванных сертификатов, считается конфиденциальной.

Информация, хранящаяся в журналах аудита УЦ, считается конфиденциальной и не подлежит разглашению.

5.2.2. Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной, является открытой информацией. К открытой информации относятся данные, включаемые в сертификаты ключей проверки электронных подписей их владельцев и списки отозванных сертификатов, издаваемые УЦ.

Открытая информация может публиковаться по решению УЦ.

5.2.3. Исключительные полномочия официальных лиц

УЦ не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев, требующих раскрытия в соответствии с действующим законодательством РФ.

5.2.4. Обработка персональных данных в УЦ

Политика обработки персональных данных, обрабатываемых в УЦ действует в отношении всех персональных данных, которые УЦ может получить от владельца сертификата.

Целью обработки персональных данных является оказание услуг УЦ возложенных законодательством Российской Федерации функций, полномочий и обязанностей.

Обработка персональных данных в УЦ осуществляется на основании согласия владельца сертификата с обработкой персональных данных в форме приложения № 1 и 2 настоящего регламента.

Персональные данные обрабатываемые в УЦ и вносимые в сертификат владельца относятся к категории общедоступных данных.

УЦ осуществляет сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение персональных данных в соответствии с Федеральным законом от 27.06.2006 №152-ФЗ «О персональных данных».

Срок обработки персональных данных при оказании услуг УЦ равен сроку деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации.

Владельцы сертификатов имеют право требовать внесения изменений и дополнений своих персональных данных, обрабатываемых в УЦ, обратившись к лицу, ответственному за организацию обработки персональных данных в УЦ, при этом они должны иметь подтверждающие документы, в соответствии с которыми вносятся изменения.

5.3. Регистрация квалифицированного сертификата владельца в ЕСИА

УЦ осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации (ЕСИА) в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

По желанию лица, которому выдан квалифицированный сертификат, УЦ безвозмездно осуществляет регистрацию квалифицированного сертификата в ЕСИА.

Приложение №1
к Регламенту УЦ
(Форма заявления на изготовление
сертификата для ЮЛ, ИП)

Заявление
на изготовление (создание) сертификата в УЦ

_____ (наименование организации, включая организационно-правовую форму)
в лице _____ (должность)

_____ (фамилия, имя, отчество)
действующего на основании _____
Просит создать ключ электронной подписи и ключ проверки электронной подписи, изготовить
(создать) сертификат владельцу _____ (фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении данными:

Должность владельца	
Фактический адрес местонахождения организации (улица, номер дома)	
ФИО владельца	
Подразделение	
Сокращённое наименование организации, согласно выписки ЕГРЮЛ (ЕГРИП)	
Город	
Область	
Страна	RU
Адрес электронной почты владельца	
ИНН/КПП организации	
ОГРН (ОГРНИП) организации	
СНИЛС владельца	

Владелец сертификата _____ (фамилия, имя, отчество)

_____ (серия и номер паспорта, кем и когда выдан)

соглашается с обработкой (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) своих персональных данных УЦ и признает, что персональные данные, заносимые в сертификат, владельцем которых он является, относятся к общедоступным персональным данным.

Ознакомлен с требованиями Регламента УЦ и приложениями к нему, в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.

Владелец сертификата _____

_____ (подпись)

_____ (фамилия, инициалы)

« ____ » _____ 201 г.

_____ (должность руководителя организации)

_____ (подпись)

_____ (фамилия, инициалы)

М.П.

« ____ » _____ 201 г.

Приложение №2
к Регламенту УЦ
(Форма заявления на изготовление
сертификата для ФЛ)

Заявление
на изготовление (создание) сертификата в УЦ

(фамилия, имя, отчество)

(номер и серия документа, удостоверяющего личность, когда и кем выдан)

Просит создать ключ электронной подписи и ключ проверки электронной подписи, изготовить (создать) сертификат в соответствии с указанными в настоящем заявлении данными:

Фактический адрес (город, улица, номер дома)	
ФИО владельца	
Город	
Область	
Страна	RU
Адрес электронной почты владельца	
ИНН владельца	
СНИЛС владельца	

Владелец сертификата _____

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) своих персональных данных УЦ и признает, что персональные данные, заносимые в сертификат, владельцем которых он является, относятся к общедоступным персональным данным.

Ознакомлен с требованиями Регламента УЦ и приложениями к нему, в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.

Владелец сертификата _____

(подпись)

(фамилия, инициалы)

« ____ » _____ 201 г.

Приложение №3
к Регламенту УЦ
(Форма заявления на аннулирование
сертификата для ЮЛ, ИП)

Заявление
на аннулирование сертификата владельца в УЦ

_____ (наименование организации, включая организационно-правовую форму)

в лице _____

_____ (должность)

_____ (фамилия, имя, отчество)
действующего на основании _____

Просит аннулировать сертификат владельца своего уполномоченного представителя

_____ (фамилия, имя, отчество)

содержащий следующие данные:

Серийный номер сертификата владельца	
Должность владельца	
ФИО владельца	
Подразделение	
Сокращённое наименование организации, согласно выписки ЕГРЮЛ (ЕГРИП)	
Город	
Область	
Страна	RU
Адрес электронной почты владельца	

Владелец сертификата _____

_____ (подпись)

_____ (фамилия, инициалы)

« ____ » _____ 201 г.

_____ (должность руководителя организации)

_____ (подпись)

_____ (фамилия, инициалы)

М.П.

« ____ » _____ 201 г.

Приложение №4
к Регламенту УЦ
 (Форма заявления на аннулирование
 сертификата для ФЛ)

Заявление
на аннулирование сертификата владельца в УЦ

_____ (фамилия, имя, отчество)

_____ (номер и серия документа, удостоверяющего личность, когда и кем выдан)

Прошу аннулировать выданный на мое имя сертификат, содержащий следующие данные:

Фактический адрес (город, улица, номер дома)	
ФИО владельца	
Город	
Область	
Страна	RU
Адрес электронной почты владельца	
ИНН владельца	
СНИЛС владельца	

Владелец сертификата _____

_____ (подпись)

_____ (фамилия, инициалы)

« ____ » _____ 201 г.

Приложение №5
к Регламенту УЦ
 (Форма заявления на подтверждение
 действительности ЭП для ЮЛ, ИП)

Заявление
на подтверждение действительности электронной подписи в электронном документе

_____ (наименование организации, включая организационно-правовую форму)

в лице _____

_____ (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Просит подтвердить действительность ЭП в электронном документе на основании следующих данных:

1. Заверенный УЦ сертификат ключа проверки электронной подписи владельца сертификата, серийный № _____;

2. Ключевой носитель, содержащий сертификат ключа проверки электронной подписи, ключ электронной подписи и ключ проверки электронной подписи, с использованием которого необходимо осуществить подтверждение действительности ЭП в электронном документе. Ключевой носитель, серийный № _____;

3. Файл, содержащий подписанные ЭП электронные документы на прилагаемом к заявлению носителе, серийный № _____;

4. Время на момент наступления которых требуется подтвердить действительность ЭП:
 « _____ : _____ » « _____ / _____ / _____ »;
 (час минута) (день месяц год)

Владелец сертификата _____

_____ (подпись)

_____ (фамилия, инициалы)

« _____ » _____ 201 г.

_____ (должность руководителя организации)

_____ (подпись)

_____ (фамилия, инициалы)

М.П.

« _____ » _____ 201 г.

Приложение №6
к Регламенту УЦ
 (Форма заявления на подтверждение
 действительности ЭП для ФЛ)

Заявление
на подтверждение действительности электронной подписи в электронном документе

(фамилия, имя, отчество)

(номер и серия документа, удостоверяющего личность, когда и кем выдан)

Прошу подтвердить действительность ЭП в электронном документе на основании следующих данных:

1. Заваренный УЦ сертификат ключа проверки электронной подписи владельца сертификата, серийный № _____;
2. Ключевой носитель, содержащий сертификат ключа проверки электронной подписи, ключ электронной подписи и ключ проверки электронной подписи, с использованием которого необходимо осуществить подтверждение действительности ЭП в электронном документе. Ключевой носитель, серийный № _____;
3. Файл, содержащий подписанные ЭП электронные документы на прилагаемом к заявлению носителе, серийный № _____;
4. Время на момент наступления которых требуется подтвердить действительность ЭП:
 « _____ : _____ » « _____ / _____ / _____ »;
 (час минута) (день месяц год)

Владелец сертификата _____

(подпись)

(фамилия, инициалы)

« _____ » _____ 201 г.

**Приложение №7
к Регламенту УЦ**

(Форма нотариальной доверенности на получение ЭП для ЮЛ, ИП)

Доверенность

г. _____ « ____ » _____ 20__ г.

(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает представителя _____
(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1. Предоставить в УЦ необходимые документы, определённые регламентом УЦ для изготовления (создания) сертификата владельцу.
2. Получить сформированный ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи на владельца сертификата

(фамилия, имя, отчество владельца сертификата)

а также иные документы, определённые регламентом УЦ.

3. Получить средства криптографической защиты информации в УЦ и выполнить все необходимые действия связанные с исполнением настоящего поручения, в т.ч. с правом подписи в журнале поэкземплярного учёта СКЗИ и прочих учётных документах.
4. Уполномоченный представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определённых настоящей доверенностью.
5. Подписать бухгалтерские документы (в рамках выполнения работ и оказания услуг по договору).

Настоящая доверенность выдана сроком на 1 (один) месяц без права передоверия.

Подпись уполномоченного представителя _____
(подпись) (фамилия, инициалы)

подтверждаю.

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

Приложение №8
к Регламенту УЦ

(Форма нотариальной доверенности на получение ЭП для ФЛ)

Доверенность

Г. _____

« ____ » _____ 20__ г.

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

уполномочиваю представителя _____

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1. Предоставить в УЦ необходимые документы, определённые регламентом УЦ для изготовления (создания) на моё имя сертификата владельца.
2. Получить для меня сформированный ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, а также иные документы, определённые регламентом УЦ.
3. Получить средства криптографической защиты информации в УЦ и выполнить все необходимые действия связанные с исполнением настоящего поручения, в т.ч. с правом подписи в журнале поэкземплярного учёта СКЗИ и прочих учётных документах.
4. Уполномоченный представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определённых настоящей доверенностью.
5. Подписать бухгалтерские документы (в рамках выполнения работ и оказания услуг по договору).

Настоящая доверенность выдана сроком на 1 (один) месяц без права передоверия.

Подпись уполномоченного представителя _____

(подпись)

(фамилия, инициалы)

подтверждаю.

Владелец сертификата _____

(подпись)

(фамилия, инициалы)

Приложение №9
к Регламенту УЦ
(Форма доверенности на право
участия в электронных торгах для ЮЛ, ИП)

Доверенность

г. _____ « ____ » _____ 20__ г.

_____ (наименование организации, включая организационно-правовую форму)

в лице _____ (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает представителя _____ (фамилия, имя, отчество)

_____ (серия и номер паспорта, кем и когда выдан)

выступать в роли владельца сертификата, с правом участия в качестве участника размещения заказа на электронных площадках, отобранных для проведения открытых аукционов в электронной форме, а также внести следующие сведения, устанавливающие правомерность использования сертификата ключа подписи его владельцем на электронных площадках:

Тип участника (подчеркнуть один вариант из списка)	ЮЛ, Индивидуальный предприниматель
Полномочия (подчеркнуть варианты из списка)	Администратор организации, Уполномоченный специалист Специалист с правом подписи контракта

Настоящая доверенность действительна по « ____ » _____ 20__ г.

Владелец ключа подписи

_____ (подпись)

_____ (фамилия, инициалы)

« ____ » _____ 201 г.

_____ (должность руководителя организации)

_____ (подпись)
М.П.

_____ (фамилия, инициалы)

« ____ » _____ 201 г.

Приложение №10
к Регламенту УЦ
 (Форма доверенности на подтверждение
 правомочия лица для ЮЛ, ИП)

Доверенность

г. _____ « ____ » _____ 20__ г.

_____ (наименование организации, включая организационно-правовую форму)

в лице _____

_____ (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает своего представителя _____

_____ (фамилия, имя, отчество)

_____ (серия и номер паспорта, кем и когда выдан)

Совершать от имени и в интересах доверителя следующие действия (операции):

1. Предоставлять в УЦ необходимые документы, определённые регламентом УЦ для изготовления (создания) сертификата на своё имя.
2. Получать сформированные ключ электронной подписи и ключ проверки электронной подписи, сертификат ключа проверки электронной подписи, а также иные документы, определённые регламентом УЦ.
3. Получать средства криптографической защиты информации в УЦ и выполнять все необходимые действия связанные с исполнением настоящего поручения, в т.ч. с правом подписи в журнале поэкземплярного учёта СКЗИ и прочих учётных документах УЦ.
4. Подписывать бухгалтерские документы (в рамках выполнения работ и оказания услуг по договору).
5. Представлять интересы доверителя перед УЦ.

Настоящая доверенность выдана сроком на 1 (один) календарный год без права передоверия.

Подпись уполномоченного представителя _____

_____ (подпись)

_____ (фамилия, инициалы)

подтверждаю.

Руководитель организации _____

_____ (подпись)

М.П.

_____ (фамилия, инициалы)