«УТВЕРЖДАЮ»
Директор ООО «МОСТИНФО»
_____ / И.Б. Вилисова
16 марта 2013 г.
Редакция от 17.06.2019 г.

Регламент Удостоверяющего Центра ООО «Мостинфо» оказания услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей

МОСТ ИНФО

Екатеринбург
2019

1. Введение

1.1. Обзорная информация

Настоящий Регламент Удостоверяющего центра ООО «Мостинфо», именуемый в дальнейшем - «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, и определяет механизмы и условия предоставления и использования услуг Удостоверяющего Центра ООО «Мостинфо» (УЦ), включая обязанности пользователей (владельцев открытых ключей подписи) и членов группы администрирования УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ, а также устанавливает общий порядок и условия предоставления удостоверяющим центром услуг по изготовлению сертификатов ключей подписи и дополнительных услуг, связанных с управлением сертификатами ключей подписи.

Настоящий Регламент является договором присоединения на основании статьи 428 Гражданского кодекса РФ.

1.2. Идентификация

Наименование документа: «Регламент Удостоверяющего Центра ООО «Мостинфо» оказания услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей».

Версия: 5.2.

Дата: 17.06.2019 г.

1.3. Распространение Регламента и рассылка информации

Настоящий Регламент размещен для свободного доступа и ознакомления для всех заинтересованных лиц в электронной форме по адресу: **http://most-info.ru/my/reglament1/**), либо получить копию Регламента через электронную почту от отправителя **info@most-info.ru** (по запросу).

Копию Регламента в бумажной форме можно получить в офисе ООО «Мостинфо» по адресу г. Екатеринбург, ул. Первомайская, д. 15, оф. 1204. Удостоверяющий Центр вправе взимать с пользователей плату за предоставление Регламента в бумажной форме, указанная плата не должна превышать расходов на изготовление копии Регламента.

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

Уведомление Пользователей УЦ о внесении изменений (дополнений) в Регламент осуществляется удостоверяющим центром путем размещения очередной редакции настоящего Регламента, включающей указанные изменения (дополнения), на сайте удостоверяющего центра по адресу: **http://most-info.ru/my/reglament1/**

1.4. Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязательства по всем вовлеченным сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.5. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента – 6 лет.

Если Удостоверяющий Центр официально не уведомит пользователей УЦ о прекращении действия Регламента, действие Регламента автоматически пролонгируется на следующие 6 лет.

Официальное уведомление о прекращении действия Регламента осуществляется на сайте компании **www.most-info.ru**.

2. Общие положения

2.1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «Мостинфо-Екатеринбург», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Екатеринбурге, свидетельство о государственной регистрации юридического лица, серия 66 № 005573120, выдано Инспекцией ФНС России по Железнодорожному району г. Екатеринбурга Свердловской области 16.05.2006 г., внесено в Единый государственный реестр юридических лиц за основным государственным номером 1069659052760, свидетельство о внесении записи в Единый государственный реестр юридических лиц в связи с государственной регистрацией изменений, вносимых в учредительные документы юридического лица, за государственным регистрационным номером 2126678168538, выдано Межрайонной инспекцией ФНС России № 24 по Свердловской области 18.10.2012 г., серия 66 № 006743537.

Свидетельство об аккредитации удостоверяющего центра рег. № 835 от 24.01.2018 г.

Удостоверяющий центр осуществляет деятельность по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей на территории Российской Федерации на основании лицензии ЛСЗ № 0007861 рег. № 514 от 20.04.2015 г., выданной Управлением Федеральной службы безопасности Российской Федерации по Свердловской области в соответствии с постановлением Российской Федерации № 313 от 16 апреля 2012 года «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

Реквизиты ООО «МОСТИНФО»:

Полное наименование: Общество с ограниченной ответственностью «Мостинфо-Екатеринбург»

Краткое наименование: ООО «МОСТИНФО»

ОГРН 1069659052760

ИНН/КПП 6659140843/ 667001001

Юридический адрес: 620075, г. Екатеринбург, ул. Первомайская, д. 15, офис 1204

Фактический адрес: 620075, г. Екатеринбург, ул. Первомайская, д. 15, офис 1204

Банковские реквизиты:
Р/счет 40702810502270001585
в Точка ПАО Банка «ФК Открытие»
БИК 044525999
Кор/счет 30101810845250000999
ОКПО 95783134
Контактные телефоны, адрес электронной почты: тел. 8 (343) 287-04-67/ 287-11-15, 8-800-707-15-02, e-mail: info@most-info.ru
Web-сайт: www.most-info.ru
График работы офиса и технической поддержки: пн.-пт. – с 09:00 до 18:00, сб.-вс. – выходной. Обед с 13:00 до 14:00
График работы обособленных подразделений указан на сайте удостоверяющего центра по адресу - **www.most-info.ru**

2.2. Термины и определения

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

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

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 (далее - проверка электронной подписи).

Реестр сертификатов – реестр квалифицированных сертификатов ключей проверки электронной подписи, включающий в себя следующие разделы:

- реестр выданных квалифицированных сертификатов ключей проверки электронной подписи;
- реестр зарегистрированных владельцев квалифицированных сертификатов ключей проверки электронных подписей.

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

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.

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов

ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

Уполномоченное лицо Удостоверяющего Центра – физическое лицо, являющееся сотрудником Удостоверяющего Центра и наделенное Удостоверяющим Центром полномочиями по заверке Сертификатов ключей подписи и Списков отозванных сертификатов.

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

Кодовая фраза – последовательность символов, используемая для аутентификации Пользователя УЦ Оператором Удостоверяющего Центра для выполнения удаленного управления сертификатом ключа подписи.

Электронная подпись (далее - 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.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security; Удостоверяющий Центр осуществляет свою работу в соответствии со следующими стандартами PKCS:

PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений; Удостоверяющий Центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;

PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

2.3. Услуги, предоставляемые Удостоверяющим Центром

Удостоверяющий Центр осуществляет свою деятельность на возмездной основе.

Список услуг, оказываемых удостоверяющим центром по Регламенту, но не ограничиваясь:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;
- осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр

сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

2.4. Разрешение споров (разбор конфликтных ситуаций)

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий Центр и пользователь УЦ.

При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Любые споры (конфликтные ситуации) между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в судебном порядке в соответствии с действующим законодательством Российской Федерации.

2.5. Платность услуг

Удостоверяющий Центр осуществляет свою деятельность на возмездной основе.

Услуга Удостоверяющего Центра по предоставлению сертификатов в форме электронных документов из реестра изготовленных сертификатов, предоставляется на безвозмездной основе.

Вознаграждение Удостоверяющего Центра по настоящему Регламенту устанавливается в соответствии с утвержденным Прейскурантом на услуги Удостоверяющего Центра. Состав и стоимость предоставляемых дополнительных услуг определяется Владельцем УЦ.

2.6. Ответственность

Удостоверяющий Центр не несет никакой ответственности в случае нарушения пользователями УЦ положений настоящего Регламента.

Удостоверяющий центр не несет ответственность за ущерб, понесенный лицом в результате доверия к сертификату, если удостоверяющий центр выполнил все требования Федерального закона № 63-ФЗ от 06 апреля 2011 года и соглашения с владельцем сертификата.

Удостоверяющий центр не несет ответственность за неисполнение или ненадлежащие исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если удостоверяющий центр

обоснованно полагался на сведения, указанные в заявлениях и других документах Пользователя УЦ или стороны присоединившейся к Регламенту.

Претензии к Удостоверяющему Центру ограничиваются указанием на несоответствие его действий настоящему Регламенту.

2.7. Прекращение деятельности

Деятельность Удостоверяющего Центра может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

2) передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным удостоверяющим центром квалифицированных сертификатов;

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

2.8. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент составляется в письменной форме и заверяется собственноручной подписью руководителя Удостоверяющего Центра и печатью Удостоверяющего Центра.

Изменения и дополнения в Регламент вносятся Удостоверяющим Центром в одностороннем порядке с обязательным уведомлением пользователей о внесении изменений на основании приказа УЦ о внесении изменений и выпуска новой редакции регламента, утверждаемой директором ООО «Мостинфо».

Изменению не подлежат положения настоящего Регламента, прямо или косвенно ущемляющие права пользователей услуг Удостоверяющего Центра.

2.9. Присоединение к Регламенту

Фактом заявления Пользователя УЦ о присоединении к настоящему Регламенту является наиболее ранний из моментов: момент отправки Пользователем УЦ через корпоративную заявочную систему УЦ ООО «Мостинфо» документов, необходимых для выпуска сертификата или момент предоставления Пользователем УЦ документов, необходимых для выпуска сертификата

С момента получения Удостоверяющим центром документов, необходимых для изготовления сертификата, Пользователь УЦ считается присоединившемся к Регламенту и является Стороной Регламента.

С момента присоединения Пользователя УЦ к настоящему Регламенту, Пользователь УЦ полностью и безоговорочно соглашается со всеми условиями настоящего Регламента и приложений к нему.

Пользователь УЦ, присоединившийся к настоящему Регламенту, самостоятельно отслеживает изменения (дополнения), вносимые в настоящий Регламент в виде его новой редакции, путем самостоятельного ознакомления с текстом Регламента на сайте удостоверяющего центра по адресу - **http://most-info.ru/my/reglament1/**.

3. Права

3.1. Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

1. Отказать в изготовлении сертификата ключа подписи Пользователя УЦ в случае непредставления документов, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение, без предоставления информации о причинах отказа
2. Отказать в изготовлении ключей не зарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;
3. Отказать в изготовлении сертификата ключа электронной подписи зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата ключа подписи, с указанием причин отказа;
4. Отказать в аннулировании (отзыве) сертификата ключа владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае если истек установленный срок действия ключа ЭП, либо в случае предоставления документов, подлинность которых вызывает сомнение;
5. Аннулировать (отозвать) сертификат ключа пользователя УЦ в случае установленного факта компрометации соответствующего ключа подписи, с уведомлением владельца, аннулированного (отозванного) сертификата ключа и указанием обоснованных причин;
6. Отказать Пользователю УЦ в исполнении услуги удаленного отзыва сертификата в случае невозможности аутентификации Пользователя УЦ;
7. Наделять третьих лиц полномочиями по вручению сертификатов ключей проверки электронных подписей от имени УЦ;
8. Выдавать сертификат ключа проверки электронной подписи, как в форме электронных документов, так и в форме документов на бумажном носителе;
9. Отказать в изготовлении сертификата ключа проверки электронной подписи, если предоставленные Заявителем сведения не прошли проверку в соответствии с п.2.2, 2.3 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
10. Отказать в изготовлении сертификата ключа подписи Заявителю в случае невыполнения заявителем обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также Регламентом УЦ;
11. Отказать в изготовлении сертификата ключа подписи Заявителя при расхождении данных, предоставленных Заявителем с данными, указанными в ЕГРЮЛ или ЕГРИП;
12. Проверять достоверность документов и сведений, предоставленных заявителем, с использованием инфраструктуры, 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.
13. Аннулировать сертификат, в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением

Владельца аннулированного сертификата ключа подписи по электронной почте, указанной при заполнении заявления на сертификат.

3.2. Права пользователей УЦ

Пользователи сертификатов ключей проверки ЭП (пользователи УЦ, не имеющие собственных сертификатов, но использующие сертификаты других пользователей УЦ для каких-либо целей) имеют следующие права:

1. Получить список аннулированных (отозванных), изготовленный Удостоверяющим Центром;
2. Получить сертификат ключа уполномоченного лица Удостоверяющего Центра;
3. Применять сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра для проверки электронной подписи уполномоченного лица Удостоверяющего Центра в сертификатах ключа, изготовленных Удостоверяющим Центром.
4. Применять ключ проверки электронной подписи в электронной форме для проверки квалифицированной электронной подписи электронного документа в соответствии со сведениями, указанными в сертификате ключа подписи.
5. Применять список аннулированных (отозванных), изготовленный Удостоверяющим Центром, для проверки статуса сертификатов ключей подписи.
6. Обратиться в Удостоверяющий Центр для внесения в реестр Удостоверяющего Центра регистрационной информации о пользователе, с целью в дальнейшем стать владельцем сертификата ключа ЭП;
7. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей в документах, представленных в электронной форме;
8. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах ключей;
9. Обратиться в Удостоверяющий Центр на предмет получения (приобретения) средства электронной подписи;
10. Сформировать ключ электронной подписи и на своем рабочем месте с использованием средства ЭП, предоставляемых Удостоверяющим Центром.
11. Обратиться в Удостоверяющий Центр с заявлением в бумажной форме на изготовление сертификата ключа ЭП;
12. Обратиться в Удостоверяющий Центр для аннулирования (отзыва) сертификата ключа ЭП в течение срока действия соответствующего ключа электронной подписи;
13. Получить под расписку от Удостоверяющего центра инструкции по обеспечению безопасности использования квалифицированной электронной подписи и Средств квалифицированной электронной подписи.

4. Обязательства

4.1. Обязательства Удостоверяющего Центра

4.1.1. Ключ подписи уполномоченного лица Удостоверяющего Центра

Удостоверяющий Центр обязан:

- использовать для изготовления ключа уполномоченного лица Удостоверяющего Центра и формирования электронной подписи только средства электронной подписи, сертифицированные в

соответствии с действующим законодательством Российской Федерации;

- использовать для подписания от своего имени квалифицированных сертификатов и списков аннулированных сертификатов, квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган;
- не использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами;
- принять меры по защите ключа ЭП уполномоченного лица Удостоверяющего Центра в соответствии с положениями настоящего Регламента.

4.1.2. Синхронизация времени

Удостоверяющий Центр организует работу своих Служб по GMT (Greenwich Mean Time) с учетом часового пояса.

Удостоверяющий Центр обязан синхронизировать по времени все программные и технические средства обеспечения деятельности по предназначению.

4.1.3. Регистрация пользователей УЦ

Удостоверяющий Центр обеспечивает регистрацию пользователей УЦ в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

Удостоверяющий Центр обязан:

- обеспечить уникальность регистрационной информации пользователей УЦ, заносимой в реестр Удостоверяющего Центра и используемой для идентификации владельцев сертификатов ключей;
- не разглашать (не публиковать) конфиденциальную информацию пользователей УЦ, за исключением информации используемой для идентификации владельцев сертификатов ключей и заносимой в изготавливаемые сертификаты.

Публикация информации, используемой для идентификации владельцев сертификатов ключей, осуществляется путем включения ее в изготавливаемые сертификаты.

4.1.4. Изготовление ключей пользователей УЦ

Удостоверяющий Центр обязан:

- изготовить ключ ЭП и ключ проверки ЭП зарегистрированному пользователю по заявлению с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством Российской Федерации;
- обеспечивать конфиденциальность созданных ключей электронных подписей;
- записать ключ на отчуждаемый носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей;
- выполнять процедуру генерации ключей и запись ключей на отчуждаемый носитель только с использованием программного и/или

аппаратного средства, сертифицированного в соответствии с законодательством Российской Федерации;
- обеспечить защиту ключевого носителя от копирования.

4.1.5. Изготовление сертификатов ключей ЭП

Удостоверяющий Центр обеспечивает изготовление сертификата ключа ЭП зарегистрированному пользователю по заявлению, в соответствии с форматом и порядком идентификации владельца сертификата ключа, определенным в настоящем Регламенте.

Удостоверяющий Центр обязан:
- обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов ключей пользователей УЦ;
- обеспечить уникальность значений ключей ЭП в изготовленных сертификатах ключей пользователей УЦ;
- отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи.

4.1.6. Аннулирование (отзыв) сертификатов ключей ЭП

Удостоверяющий Центр обязан:
- аннулировать (отозвать) сертификат ключа по заявлению его владельца;
- в течение 30 минут с момента получения заявления владельца сертификата занести сведения об аннулированном (отозванном) сертификате в список аннулированных сертификатов с указанием даты и времени занесения и причины отзыва.

4.1.7. Уведомления

4.1.7.1. Уведомление о факте аннулирования сертификата ключа ЭП.

Удостоверяющий Центр обязан:
- официально уведомить о факте аннулирования (отзыва) сертификата ключа его владельца, путем направления электронного документа по электронной почте, указанной в заявлении на изготовление сертификата до внесения в реестр сертификатов информации об аннулировании;
- включать полный адрес (URL) списка аннулированных сертификатов из репозитория Удостоверяющего Центра в издаваемые сертификаты открытых ключей пользователей УЦ.

Срок уведомления в течение 30 минут с момента получения сведений о наличии оснований для прекращения их действия (аннулирования) и занесения сведений об аннулированном (отозванном) сертификате в список аннулированных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка аннулированных сертификатов, содержащим сведения об аннулированном (отозванном) сертификате, в репозитории Владельца УЦ.

Временем аннулирования (отзыва) сертификата ключа подписи признается время опубликования списка аннулированных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате.

Временем опубликования списка аннулированных сертификатов признается время публикации списка аннулированных сертификатов в репозитории Владельца УЦ.

4.1.8. Реестр сертификатов ключей

Реестр сертификатов ключей ведется в электронном виде.

Сертификаты ключей представлены в реестре в форме электронных копий изготовленных сертификатов.

Выписка из реестра Удостоверяющего Центра предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определенном настоящим Регламентом.

Удостоверяющий Центр обязан:

- вести реестр всех изготовленных сертификатов ключей пользователей УЦ в течение установленного срока хранения;
- вносить информацию о сертификате ключа проверки электронной подписи в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата;
- обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов УЦ в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами;
- осуществлять выдачу копий сертификатов ключей в электронной форме по обращениям пользователей УЦ;
- публиковать выписки из реестра, позволяющие определить действительность сертификатов ключей пользователей УЦ;
- вносить информацию о прекращении действия сертификата ключа проверки электронной подписи в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

4.1.9. Прочие обязательства

Удостоверяющий Центр обязан:

- информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;
- уведомлять владельца сертификата ключа о фактах, которые стали известны Удостоверяющему Центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа;

- соблюдать требования, на соответствие которым аккредитован, в течение всего срока аккредитации. В случае возникновения обстоятельств, делающих невозможным соблюдение указанных требований, УЦ немедленно уведомляет об этом в письменной форме уполномоченный федеральный орган;
- выполнять порядок реализации функций УЦ и исполнять обязанности УЦ, установленные настоящим Регламентом;
- осуществить присоединение информационной системы, обеспечивающей реализацию функций аккредитованного УЦ к информационно-технологической и коммуникационной инфраструктуре в порядке, установленном в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг";
- при выдаче квалифицированного сертификата ключа проверки электронной подписи установить личность заявителя – физического лица, обратившегося за получением квалифицированного сертификата ключа проверки электронной подписи;
- получить от лица, выступающего от имени заявителя – юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;
- ознакомить Заявителя под расписку с информацией, содержащейся в квалифицированном сертификате при выдаче квалифицированного сертификата ключа проверки электронной подписи;
- одновременно с выдачей квалифицированного сертификата выдать владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
- направлять в единую систему идентификации и аутентификации сведения о лице, получившем 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 лица, которому выдан квалифицированный сертификат безвозмездно осуществлять регистрацию лица в единой системе идентификации и аутентификации при выдаче квалифицированного сертификата;
- вносить в сертификат ключа проверки электронной подписи только достоверную информацию, подтвержденную соответствующими документами.

При прекращении деятельности УЦ обязан:

- сообщить в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;
- передать в уполномоченный федеральный орган в установленном порядке реестр выданных УЦ квалифицированных сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в УЦ.

Удостоверяющий Центр обязан хранить информацию, указанную в части 1 статьи 15 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», в течение срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, в форме, позволяющей проверить ее целостность и достоверность, а именно:

- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

4.2. Обязательства пользователей УЦ

4.2.1. Обязанности лиц, проходящих процедуру регистрации

Лица, проходящие процедуру регистрации в реестре Удостоверяющего Центра, обязаны:

- представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента;
- при подаче заявления на сертификат ключа проверки электронной подписи указать действующий электронный почтовый адрес владельца сертификата ключа проверки электронной подписи для получения извещений, уведомлений от УЦ, связанных с применением сертификата ключа проверки электронной подписи, его аннулированием;
- использовать для создания и проверки квалифицированных электронных подписей, создания Ключей квалифицированных электронных подписей и Ключей их проверки Средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с 63-ФЗ;

4.2.2. Обязанности владельца ключа электронной подписи

Владелец ключа ЭП обязан:

- хранить в тайне ключ ЭП, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
- обеспечить конфиденциальность ключа электронной подписи. Не использовать ключ электронной подписи и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- не использовать ключи электронной подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;
- использовать ключ электронной подписи только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;
- извещать Удостоверяющий Центр обо всех изменениях данных, внесенных в

сертификат;

- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован, или заявление на аннулирование, которого подано в Удостоверяющий Центр в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата по момент времени официального уведомления об аннулировании сертификата.

4.2.3. Обязанности владельца сертификата ключа проверки электронной подписи

Владелец сертификата ключа проверки электронной подписи, изданного Удостоверяющим Центром, обязан:

- использовать сертификат ключа только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;
- немедленно обратиться в Удостоверяющий Центр с заявлением на аннулирование (отзыв) сертификата ключа в случае, если ему известно, что эти ключи используются или использовались ранее другими лицами.

4.2.4. Обязанности пользователей сертификатов ключей проверки электронной подписи

Перед тем как использовать сертификат ключа проверки электронной подписи, изготовленный Удостоверяющим Центром, пользователь сертификата (пользователь, не являющийся его владельцем) должен удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту, соответствует предполагаемому использованию.

5. Политика конфиденциальности

5.1. Типы конфиденциальной информации

Типы информации, являющиеся конфиденциальной:

Закрытый ключ, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией Пользователя УЦ. Удостоверяющий центр не осуществляет хранение закрытых ключей Операторов и Пользователей УЦ.

Типы информации, не являющейся конфиденциальной:

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации открытой информации определяется УЦ.

Информация, включаемая в списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной.

11.2. Исключительные полномочия Удостоверяющего центра:

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

11.3. Обработка персональных данных пользователей удостоверяющего центра:

Цель обработки персональных данных УЦ - идентификация и аутентификация субъекта персональных данных в качестве пользователя УЦ, а

также пользователя информационных систем с применением ЭП, в которых используются сертификаты ключей подписи Пользователя УЦ.

Обработка персональных данных в УЦ осуществляется на основании согласия владельца сертификата.

Пользователь не может быть зарегистрирован в реестре УЦ в порядке, установленном настоящим Регламентом, без заключения договора, а также без согласия на обработку персональных данных.

Персональные данные, обрабатываемые УЦ: фамилия, имя, отчество, паспортные данные, СНИЛС, идентификационный номер налогоплательщика владельца сертификата. В сертификат ключа подписи, изготавливаемый УЦ, вносят фамилию, имя, отчество, СНИЛС, идентификационный номер налогоплательщика.

Персональные данные, вносимые в сертификат ключа проверки электронной подписи относятся к категории общедоступных.

УЦ осуществляет действия по сбору, записи, систематизации, накоплению, использованию, хранению, уточнению, обновлению, изменению, блокированию и уничтожению персональных данных Пользователя УЦ в соответствии с Федеральным законом от 27.06.2006 г. № 152-ФЗ «О персональных данных»

Удостоверяющий центр не раскрывает третьим лицам и не распространяет персональные данные Пользователя УЦ без наличия письменного его согласия на раскрытие данной информации, за исключением случаев, прямо установленных действующим законодательством Российской Федерации.

Согласие на обработку персональных данных пользователя УЦ может быть отозвано по письменному заявлению пользователя УЦ, при удовлетворении которого в последствии Удостоверяющим центром отзываются все выпущенные сертификаты данного Пользователя УЦ.

5.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией является открытой информацией.

Открытая информация может публиковаться по решению Удостоверяющего Центра.

Место, способ и время публикации также определяется решением Удостоверяющего Центра.

Информация, включаемая в сертификаты открытых ключей пользователей УЦ и списки отозванных сертификатов, издаваемые Удостоверяющим Центром, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

5.3. Исключительные полномочия официальных лиц

Удостоверяющий Центр не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

6. Процедуры и механизмы

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

Регистрация пользователя УЦ в централизованном режиме осуществляется сотрудником Службы Регистрации УЦ на основе заявления при условии установления личности Заявителя, и (или) при личном прибытии лица проходящего процедуру регистрации, в офис Удостоверяющего Центра, расположенный по адресу г. Екатеринбург, ул. Первомайская, д. 15, оф. 1204.

Сотрудник Службы Регистрации УЦ, либо доверенное лицо Удостоверяющего центра выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по основному документу, удостоверяющему личность (паспорту гражданина Российской Федерации).

После положительной идентификации лица, проходящего процедуру регистрации, Заявитель заполняет и заверяет заявление собственноручной подписью, после чего, передает заявление на регистрацию вместе с необходимыми приложениями сотруднику Службы Регистрации УЦ, либо уполномоченному лицу для дальнейшей передачи в УЦ. В случае, если заявление подается от имени юридического лица и (или) ИП, на заявлении необходимо наличие цветного оттиска печати организации.

Заявление на регистрацию рассматривается Службой Регистрации УЦ в течение 3 рабочих дней с момента поступления.

В случае отказа в регистрации заявление на регистрацию вместе с приложениями возвращается заявителю.

При принятии положительного решения, сотрудник Службы Регистрации УЦ выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего Центра.

Создание ключей электронной подписи и ключей проверки электронной подписи осуществляется одним из способов:

1) Создание Ключей электронной подписи и ключей проверки электронной подписи осуществляется в лицензированной точке выдачи Удостоверяющего Центра.
   Ключ ЭП и соответствующий ему ключ проверки ЭП могут быть изготовлены в удостоверяющем центре на специализированном рабочем месте, аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, которое размещено в аттестованном помещении лицензированной точки выдачи, доступ в которое ограничен.
2) Создание Ключей электронной подписи осуществляется пользователем УЦ самостоятельно на своем рабочем месте, при этом пользователь УЦ создает Ключ электронной подписи на своем рабочем месте с использованием предоставленных Удостоверяющим центром либо собственных Средств электронной подписи.

Изготовление ключей электронной подписи и ключей проверки электронной подписи предназначенных для создания и проверки усиленной квалифицированной электронной подписи создаются с использованием средств ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Одновременно с изготовлением ключей подписи производится формирование файла с запросом на сертификат ключа подписи зарегистрированного пользователя УЦ в формате PKCS#10.

Данные о пользователе УЦ, содержащиеся в запросе на сертификат ключа подписи пользователя УЦ, должны совпадать с данными, указанными в заявлении на изготовление сертификата ключа подписи пользователя УЦ. Невыполнение этого условия служит безусловной причиной для отказа в изготовлении сертификата ключа подписи пользователя УЦ.

В случае если изготовление ключей подписи пользователя УЦ осуществляется сотрудником Службы Регистрации, ключи, записанные на ключевой носитель, выдаются пользователю УЦ по окончании процедуры изготовления сертификата ключа подписи этого пользователя УЦ.

По окончании процедуры регистрации, зарегистрированному пользователю УЦ выдаются:

- ключи, записанные на ключевой носитель;
- сертификат ключа проверки ЭП в электронной форме, соответствующий ключу ЭП;
- сертификата ключа проверки ЭП на бумажном носителе, по форме определенной настоящим Регламентом;
- сертификатов ключа проверки ЭП в электронной форме уполномоченного лица Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии;
- списки отозванных сертификатов в электронной форме Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии.

Указанные выше данные, передаваемые зарегистрированному пользователю в электронной форме, записываются в виде файлов на отчуждаемый носитель.

По необходимости (в случае его отсутствия у пользователя), регистрируемый пользователь УЦ должен приобрести (получить) средство электронной подписи и шифрования, распространяемое Удостоверяющим Центром. Стоимость носителя определяется на основании прейскуранта, действующего на момент подачи заявления на регистрацию.

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

Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ. Плановая смена ключей ЭП производится по следующим основаниям:

- истечение срока действия сертификата ключа проверки электронной подписи;
- переход на использование новых стандартов ЭП и функции хеширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования электронной подписи.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

1. УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;

2.УЦ изготавливает новый сертификат ключа проверки электронной подписи Уполномоченного лица УЦ.

При плановой замене ключа ЭП УЦ все Владельцы должны установить на своих компьютерах новый сертификат УЦ.

Информирование Заявителей/Владельцев о проведении плановой смены ключей уполномоченного лица удостоверяющего центра осуществляется посредством публикации информации на официальном сайте удостоверяющего центра по адресу: https://most-info.ru.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте удостоверяющего центра по адресу: https://most-info.ru, доступная для скачивания.

Старый ключ ЭП УЦ используется в течение своего срока действия для формирования списков аннулированных сертификатов, изданных УЦ в период действия старого ключа ЭП УЦ.

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

Внеплановая смена ключей выполняется в следующих случаях:

- закрытый ключ УЦ закончил свой срок действия, а плановая смена произведена не была;
- произошла компрометация закрытого ключа УЦ;
- есть подозрение, что закрытый ключ УЦ мог быть скомпрометирован;
- закрытый ключ УЦ не доступен (ключевой носитель поврежден, уничтожен и т.д.);
- в связи с необходимостью внести изменение в содержимое сертификата открытого УЦ (введение новых Требований к форме или формату сертификата и т.д.);
- по решению, вступившему в законную силу (по решению суда, по решению владельца удостоверяющего центра и т.д.).

Актуальными угрозами нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра являются:

- угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к рабочим местам автоматизированной системы удостоверяющего центра.

К случаям нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра относятся в том числе:

- физическая утеря/кража носителя ключа электронной подписи Удостоверяющего центра;
- несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации или подозрение, что данные факты имели место (срабатывание сигнализации с подтверждением несанкционированного вскрытия помещения, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- иные случаи компрометации.

Процедура внеплановой смены ключей УЦ выполняется в порядке, определённом процедурой плановой смены ключей УЦ. В случае компрометации ключа ЭП УЦ сертификат УЦ аннулируется, Владельцы уведомляются об указанном факте путем публикации информации о компрометации на сайте УЦ по адресу: https://most-info.ru. Все сертификаты, подписанные с использованием скомпрометированного ключа УЦ, считаются аннулированными, с занесением

соответствующих сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов. Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте удостоверяющего центра по адресу: https://most-info.ru, доступная для скачивания.

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

Смена ключа ЭП владельца квалифицированного сертификата осуществляется в случаях:

- в связи с истечением установленного срока действия сертификата ключа проверки электронной подписи;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи;
- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи;
- 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.

6.4.1. Требования к заявлению на изготовление ключа электронной подписи

При смене сертификата Владелец подает заявление на изготовление ключа проверки ЭП в соответствии с требованиями к заявлению, указанным в п.6.5.2. настоящего Регламента.

При смене ключа ЭП владельца квалифицированного сертификата, заявление на изготовление сертификата ключа проверки электронной подписи может быть создано в форме электронного документа, подписанного усиленной квалифицированной подписью Владельца. При этом, в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, такое заявление должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата.

6.4.2. Процедура выдачи квалифицированного сертификата и ключа электронной подписи

При выдаче квалифицированного сертификата УЦ:

- устанавливает личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

- получает от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;
- ознакамливает под расписку с информацией, содержащейся в сертификате ключа проверки электронной подписи;
- выдает владельцу сертификата ключа проверки электронной подписи руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств ЭП, об условиях и о порядке использования электронных подписей и средств электронной подписи (средства криптографической защиты информации), о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей;
- направляет в единую систему идентификации и аутентификации сведения о лице, получившем 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);
- безвозмездно осуществляет регистрацию лица, которому выдан квалифицированный сертификат, в единой системе идентификации и аутентификации по его желанию.

6.5. Процедура создания и выдачи квалифицированных сертификатов

Изготовление квалифицированных ключей подписи осуществляется Удостоверяющим Центром по обращению пользователей. Обращение пользователей оформляется в форме заявления на изготовление ключей.

6.5.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

Изготовление сертификата ключа проверки электронной подписи осуществляется Удостоверяющим Центром на основании заявления на изготовление сертификата ключа зарегистрированного пользователя УЦ.

Заявление на изготовление квалифицированного сертификата ключа подписи подается заявителем в простой письменной форме на бумажном носителе и заверяется собственноручной подписью заявителя, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью. Заявление на изготовление сертификата ключа подписи оформляется заявителем либо по образцу, предоставляемому Службой Безопасности УЦ либо по бланку, подготавливаемому сотрудником Службы Безопасности УЦ.

Заявление на изготовление сертификата ключа в электронной форме подается зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, предоставляемым Удостоверяющим Центром.

Заявление на изготовление сертификата ключа в бумажной форме подается зарегистрированным пользователем УЦ в офис Службы Безопасности УЦ лично.

Срок рассмотрения заявления на изготовление сертификата ключа составляет 3 рабочих дня с момента его поступления в Службу Безопасности УЦ.

6.5.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

Форма заявления предоставляется клиенту в электронном виде. Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия.

Форма заявления на изготовление сертификата ключа проверки электронной подписи включает следующие сведения в зависимости от статуса заявителя.

Для владельца - юридического лица:

- наименование организации;
- сведения об уполномоченном представителе:
  - ФИО;
  - паспортные данные - серия, номер паспорта, дата выдачи, кем выдан, регистрация;
  - СНИЛС;
  - адрес электронной почты;
  - контактный телефон;
  - должность;
  - подразделение.
- ИНН, КПП, ОГРН;
- юридический адрес с указанием области;
- область применения ЭП.

Для владельца - индивидуального предпринимателя:

- наименование;
- ИНН, ОГРНИП;
- область, город/населенный пункт (согласно сведениям, об адресе места нахождения индивидуального предпринимателя);
- сведения об уполномоченном представителе - владельце сертификата:
  - ФИО;
  - паспортные данные - серия, номер паспорта, дата выдачи, кем выдан, регистрация;
  - СНИЛС;
  - адрес электронной почты;
  - контактный телефон;
- область применения ЭП.

Для владельца - физического лица:

- ФИО;
- паспортные данные - серия, номер паспорта, дата выдачи, кем выдан, регистрация;
- СНИЛС;
- ИНН;
- адрес электронной почты;
- контактный телефон;
- область применения ЭП.

Использование факсимиле (клише подписи) на заявлении не допускается.

6.5.3. 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, Удостоверяющий центр 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.

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

Все документы на иностранном языке должны иметь заверенный перевод на русский язык.

Требования к паспорту получателя:

- паспорт гражданина РФ не должен быть просрочен, паспорт меняется в возрасте 20 и 45 лет;
- документ не должен быть поврежден или испорчен;
- данные в документе должны совпадать с данными, указанными в доверенности на получение ЭП.

С целью исключения противоправных мошеннических действий с сертификатами ключей проверки электронной подписи, исполнения Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (при выдаче квалифицированного сертификата обязан установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата (пп.1 п.1 статьи 18 63-ФЗ), для подтверждения осуществления определенных действий, а именно, получение квалифицированного сертификата ключа проверки электронной подписи конкретным лицом, УЦ запрашивает фотографию заявителя в анфас совместно с разворотом 2-3 страницы паспорта и фотографию заявителя в анфас совместно с заявлением на изготовление сертификата ключа проверки электронной подписи.

6.5.4. Перечень документов, предоставляемых в Удостоверяющий центр

Заявитель, присоединяясь к настоящему Регламенту, предоставляет в Удостоверяющий центр следующие документы либо их надлежащим образом заверенные копии и сведения в зависимости от статуса:

Для юридических лиц:

- заявление на изготовление сертификата ключа проверки электронной подписи;
- основной государственный регистрационный номер заявителя (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);
- номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);
- основной документ, удостоверяющий личность владельца;
- основной документ, удостоверяющий личность получателя;

- номер страхового свидетельства государственного пенсионного страхования заявителя – физического лица;
- доверенность или иной документ, подтверждающие полномочия владельца сертификата ключа подписи (в случае, если владелец сертификата не имеет права действовать от лица юридического лица без доверенности);
- доверенность на получение сертификата ключа подписи (в случае, если сертификат получает сотрудник организации, не имеющий право действовать без доверенности);
- фотографию уполномоченного представителя в анфас совместно с разворотом 2-3 страницы паспорта;
- фотографию уполномоченного представителя в анфас совместно с заявлением на изготовление сертификата ключа проверки электронной подписи.

Для индивидуальных предпринимателей:

- заявление на изготовление сертификата ключа проверки электронной подписи;
- основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);
- основной документ, удостоверяющий личность владельца сертификата;
- основной документ, удостоверяющий личность получателя;
- номер страхового свидетельства государственного пенсионного страхования заявителя - физического лица;
- доверенность на получение сертификата ключа подписи (в случае, если сертификат получает не Индивидуальный предприниматель);
- фотографию уполномоченного представителя в анфас совместно с разворотом 2-3 страницы паспорта;
- фотографию уполномоченного представителя в анфас совместно с заявлением на изготовление сертификата ключа проверки электронной подписи.

Для физических лиц:

- заявление на изготовление сертификата ключа проверки электронной подписи;
- основной документ, удостоверяющий личность владельца сертификата;
- номер страхового свидетельства государственного пенсионного страхования заявителя - физического лица;
- идентификационный номер налогоплательщика заявителя;
- доверенность, подтверждающая право заявителя действовать от имени других лиц;
- фотографию уполномоченного представителя в анфас совместно с разворотом 2-3 страницы паспорта;
- фотографию уполномоченного представителя в анфас совместно с заявлением на изготовление сертификата ключа проверки электронной подписи.

В случае, если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в Удостоверяющий центр документ соответствующей формы.

6.5.5. Порядок проверки достоверности документов и сведений, представленных заявителем

УЦ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем. Для заполнения квалифицированного сертификата Удостоверяющий центр запрашивает и получает 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.

УЦ оставляет за собой право запросить у стороны, присоединившейся к Регламенту, дополнительные документы, в случае предусмотренного законодательством установления операторами государственных, муниципальных информационных систем, а также иных информационных систем общего пользования, дополнительных требований к сертификату ключа проверки электронной подписи пользователей соответствующих информационных систем для обеспечения информационной безопасности.

В случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в квалифицированный сертификат, и УЦ установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, на обращение за получением квалифицированного сертификата, УЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае, УЦ отказывает Заявителю в выдаче квалифицированного сертификата.

6.5.6. Порядок создания и выдачи квалифицированного сертификата

Изготовление ключей выполняется ответственным сотрудником Службы Безопасности УЦ на специализированном рабочем месте, на основании принятого заявления в присутствии заявителя, только после проверки и подтверждения достоверности сведений, указанных в заявлении на изготовление сертификата ключа проверки электронной подписи и представленных документов.

Изготовленные ключи записываются на ключевой носитель, предоставляемый заявителем, либо полученным в Удостоверяющем центре.

Ключевой носитель должен удовлетворять следующим требованиям:

- иметь тип устройства, входящий в перечень, определяемый Службой Безопасности УЦ;
- быть проинициализированным (отформатированным);
- не содержать никакой информации, за исключением данных инициализации.

Ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой информации не принимаются.

Ключевой носитель, содержащий изготовленные ключи, передается владельцу (заявителю), после ознакомления с информацией, содержащейся в сертификате. Факт выдачи ключей заносится в Журнал учета изготовления и выдачи ключей под роспись владельца.

В случае формирования ключа электронной подписи клиентом самостоятельно на своем персональном компьютере, сертификат ключа проверки электронной подписи выпускается на основании запроса на сертификат полученного от заявителя, только после проверки сведений, указанных в запросе.

Изготовленный сертификат передается владельцу, после ознакомления с информацией, содержащейся в сертификате.

УЦ одновременно с выдачей сертификата ключа проверки электронной подписи выдает руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

6.5.7. Срок создания и выдачи квалифицированного сертификата с момента получения Удостоверяющим центром соответствующего заявления, а также условия для срочного создания и выдачи квалифицированного сертификата заявителю

Создание Сертификата производится в течение не более трех рабочих дней с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении и соблюдения порядка оплаты за услуги.

Возможно создание сертификата в течении часа с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении, предоставлении полного пакета запрашиваемых документов, оплате путем полной предоплаты за услуги и личной явки будущего владельца сертификата ключа проверки электронной подписи за его получением.

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

6.6.1. Требования к заявлению на подтверждение действительности электронной подписи, в том числе перечень прилагаемых к такому заявлению документов

Подтверждение электронной подписи в электронном документе осуществляется Удостоверяющим Центром по обращению граждан (далее по тексту раздела - заявитель), на основании заявления на подтверждение электронной подписи в электронном документе в простой письменной форме.

Заявление на подтверждение электронной подписи в электронном документе подается заявителем в офис Административной Службы УЦ лично.

Заявление на подтверждение электронной подписи в электронном документе должно содержать информацию от заявителя о дате и времени формирования электронной подписи в электронном документе.

Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя.

Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является носитель, содержащий следующие файлы:

- Файл, содержащий электронный документ, к которому применена электронная подпись;
- Файл, содержащий электронную подпись формата PKCS#7 электронного документа, к которому применена электронная подпись;
- Файл, содержащий сертификат ключа подписи уполномоченного лица

Удостоверяющего Центра, являющегося издателем сертификата ключа подписи электронной подписи электронного документа;

Файл, содержащий список аннулированных сертификатов Удостоверяющего Центра, являющегося издателем сертификата ключа подписи электронной подписи электронного документа, и использовавшийся для проверки электронной подписи электронного документа заявителем.

6.6.2. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе

Срок рассмотрения заявления на подтверждение электронной подписи в электронном документе составляет 5 рабочих дней с момента его поступления в Административную Службу УЦ.

6.6.3. Порядок оказания услуги

В случае отказа от подтверждения электронной подписи в электронном документе заявителю возвращается заявление на подтверждение электронной подписи в электронном документе с резолюцией ответственного сотрудника Административной Службы УЦ.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи в электронном документе заявителю предоставляется ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Административной Службы УЦ и печатью Удостоверяющего Центра.

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе;
- детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

6.7. Процедуры, осуществляемые при прекращении действия и аннулирования квалифицированного сертификата

6.7.1. Основания прекращения действия или аннулирования квалифицированного сертификата

Квалифицированный сертификат прекращает свое действие в случаях:

1) Истечении срока его действия.

2) По заявлению Заявителя, подаваемому в форме документа на бумажном носителе или в форме электронного документа, при:

- смене/увольнении уполномоченного лица;
- смене реквизитов владельца;
- поломке ключевого носителя;
- утере, краже и иной компрометации ключа;
- ошибки в реквизитах или применениях.

3) В случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4) Если не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате.

5) Если установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате.

6) В случае вступления в силу решения суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию.

7) иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Владельцем.

6.7.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) квалицированного сертификата

Аннулирование (отзыв) сертификата ключа электронной подписи, изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на отзыв сертификата ключа его владельца (далее по тексту раздела заявитель).

Заявление на отзыв сертификата ключа подается заявителем в Службу Безопасности УЦ лично, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

Срок внесения информации об аннулировании сертификата в Реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

6.7.2.1. Заявление на отзыв сертификата ключа

Заявление на отзыв сертификата ключа подписи в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер отзываемого сертификата;
- Причину отзыва сертификата;
- Дата и подпись заявителя.

6.8. Порядок ведения реестра квалифицированных сертификатов

6.8.1. Формы ведения реестра квалифицированных сертификатов

Реестр сертификатов ключей проверки ЭП ведётся в электронной форме.

Ведение реестра квалифицированных сертификатов включает в себя:

- внесение изменений в реестр квалифицированных сертификатов в случае изменения сведений;
- внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Хранение информации, содержащейся в реестре квалифицированных сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

Аккредитованный удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов.

Аккредитованный удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

Формирование и ведение реестра квалифицированных сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

Аккредитованный удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре квалифицированных сертификатов.

Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре, формируется его резервная копия.

6.8.2. Сроки внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов

Срок внесения информации об аннулировании сертификата в Реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении

таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

6.9. Порядок технического обслуживания реестра квалифицированных сертификатов

6.9.1. Максимальные сроки проведения технического обслуживания

Плановое и внеплановое техническое обслуживание Реестра сертификатов осуществляется, как правило, во внерабочее время УЦ и не может превышать 12 (двенадцати) часов.

6.9.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

УЦ оповещает лиц, использующих Реестр сертификатов, о проведении планового или внепланового технического обслуживания Реестра сертификатов на официальном сайте УЦ.

6.10. Процедура подтверждения электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа подписи

Подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи осуществляется Удостоверяющим Центром по обращению пользователей (далее по тексту раздела, заявитель), на основании заявления на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи в простой письменной форме.

Заявление на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи подается заявителем в офис Административной Службы УЦ лично.

Обязательным приложением к заявлению на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа подписи является магнитный носитель (дискета 3.5.), содержащий следующие файлы:

- Файл, содержащий сертификат ключа электронной подписи зарегистрированного пользователя УЦ, подвергающийся процедуре проверки;
- Файл, содержащий сертификат ключа электронной подписи уполномоченного лица Удостоверяющего Центра, являющегося издателем сертификата ключа подписи пользователя УЦ, подвергающегося процедуре проверки;
- Файл, содержащий список аннулированных сертификатов Удостоверяющего Центра, являющегося издателем сертификата ключа электронной подписи, и использовавшийся для проверки электронной подписи уполномоченного лица Удостоверяющего Центра заявителем.

Срок рассмотрения заявления на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи составляет 5 рабочих дня с момента его поступления в Административную Службу УЦ.

В случае отказа от подтверждения электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи

заявителю возвращается заявление на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи с резолюцией ответственного сотрудника Административной Службы УЦ.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа электронной подписи заявителю предоставляется ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Административной Службы УЦ и печатью Удостоверяющего Центра.

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи уполномоченного лица Удостоверяющего Центра на сертификате ключа электронной подписи и отсутствия искажений в подписанном данной электронной подписью сертификате ключа подписи;
- детальный отчет по выполненной проверке.

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

6.11. Механизм доказательства обладания ключом электронной подписи, соответствующим ключу проверки электронной подписи

Заявления на изготовление сертификатов ключей электронной подписи, поступающие в Удостоверяющий Центр от владельцев ключей ЭП, должны содержать собственноручную подпись заявителя и в качестве реквизита запрос на сертификат, подготовленный в соответствии с форматом криптографических сообщений PKCS#10 в формате Base64 с заголовком или без оного.

Подтверждение электронной подписи запроса на сертификат из заявления на изготовление сертификатов ключей электронной подписи и наличие собственноручной подписи заявителя подтверждает, что заявитель является владельцем ключа ЭП, соответствующему ключу проверки ЭП из заявления на изготовление сертификатов ключей.

7. Порядок исполнения обязанностей Удостоверяющего центра

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

УЦ одновременно с выдачей сертификата ключа проверки электронной подписи выдает руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

7.2. Выдача по обращению заявителя средств электронной подписи

УЦ по обращению заявителя выдает средства электронной подписи, обеспечивающие выполнение следующих процедур:

- Генерацию ключей электронной подписи и ключей проверки электронной подписи;
- Формирование электронной подписи;
- Проверку электронной подписи.

Средство электронной подписи должно обеспечивать выполнение мер защиты ключей (см. раздел 7.5), а также возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

В качестве средства электронной подписи пользователи должны использовать сертифицированные в соответствии с правилами сертификации средства криптографической защиты информации по уровню защиты не ниже «КС1».

Средства криптографической защиты информации должны быть разработаны в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

Средства криптографической защиты информации должны удовлетворять по форматам и параметрам криптографических алгоритмов требованиям, изложенных в документе "Рекомендации к средствам криптографической защиты информации на взаимодействие удостоверяющих центров, реестров сертификатов, сертификаты ключей формата X.509 и электронные документы формата CMS", разработанного ООО "Крипто-Про". Авторские права подтверждены заявкой № 2001129024 ("Цифровой сертификат ключа подписи"), зарегистрированной в Российском агентстве по патентам и товарным знакам.

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

УЦ обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов, защиту информации от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий. Актуальность обеспечивается путем своевременного внесения записи о выпуске и аннулировании сертификата ключа проверки электронной подписи в реестр квалифицированных сертификатов. Режим защиты является общим требованием в отношении всей сферы применения электронной подписи, он обеспечивается посредством применения специальных шифровальных средств, способствующих защите информации от несанкционированного доступа.

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

УЦ обеспечивает доступность реестра квалифицированных электронных подписей круглосуточно, с использованием информационно-телекоммуникационных сетей к выданным УЦ квалифицированным сертификатам (https://most-info.ru/support/), за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

Ключи электронной подписи пользователей УЦ должны записываться при их генерации на отчуждаемые (относительно рабочего места) носители ключевой информации.

В качестве таких носителей ключевой информации допускается использовать только носители, указанные в формуляре средства электронной подписи, использовавшегося при их генерации.

Ключи электронной подписи на носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, учитывая следующие требования:

- Длина пароля (ПИН-кода) не должна быть меньше 6 символов;
- Пароль (ПИН-код) должен содержать символы цифр и букв латинского алфавита.

Если процедуру генерации ключей пользователя УЦ выполняет сотрудник Удостоверяющего Центра, то он должен сообщить сформированный пароль (ПИН-код) владельцу закрытых ключей.

Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца закрытых ключей.

Не допускается использовать одно и тоже значение пароля (ПИН-кода) для защиты нескольких закрытых ключей.

Сотрудники Удостоверяющего Центра, являющиеся владельцами закрытых

ключей, также выполняют указанные в разделе меры защиты закрытых ключей.

Запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется средство криптографической защиты информации, средства усиленной квалифицированной электронной подписи, после ввода ключевой информации;
- вносить какие-либо изменения в программное обеспечение средств криптографической защиты информации;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным; д. использовать ключевые носители в режимах, не предусмотренных функционированием средств криптографической защиты информации;
- записывать на ключевые носители постороннюю информацию;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами криптографической защиты информации;
- ключи ЭП на ключевом носителе защищаются паролем (пин-кодом);
- оставлять без присмотра ключи ЭП на ключевом носителе (на столе, подключенным к ПЭВМ и пр.);
- допускать использование принадлежащих им ключей электронных подписей без их согласия;
- применять ключ квалифицированной электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец несет персональную ответственность за хранение личных ключевых носителей.

Запрещается оставлять без контроля вычислительные средства с установленным средствами криптографической защиты информации после ввода ключевой информации.

В случае централизованного хранения ключевых носителей в организации, эксплуатирующей средства криптографической защиты информации, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

После плановой смены ключей или компрометации ключей Пользователи УЦ обязаны уничтожить выведенные из действия ключи электронной подписи не позднее, чем через одни сутки после момента уведомления Удостоверяющим центром о выводе ключей из действия.

Ключевая информация на носителях уничтожается путем переформатирования с использованием СКЗИ «КриптоПро CSP». Допускается данные носители после переформатирования использовать в дальнейшем Пользователями УЦ при условии записи на них новой ключевой информации.

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

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр направляет в единую систему идентификации и

аутентификации сведения о лице, получившем 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).

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

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

7.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов.

УЦ обеспечивает доступность реестра квалифицированных электронных подписей круглосуточно, с использованием информационно-телекоммуникационных сетей к выданным УЦ квалифицированным сертификатам (https://most-info.ru/support/), за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

Также УЦ публикует перечень прекративших свое действие (аннулированных) квалифицированных сертификатов, позволяющий определить действительность сертификатов ключей проверки ЭП Владельцев на официальном сайте https://most-info.ru.

7.9. Сроки действия ключей электронной подписи и сертификатов ключей электронной подписи владельцев сертификатов ключей

Максимальный срок действия ключа электронной подписи пользователя УЦ, соответствующего сертификату ключа проверки электронной подписи, владельцем которого он является, составляет 1 год 3 месяца. Начало периода действия ключа электронной подписи пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи пользователя УЦ.

Срок действия ключа электронной подписи устанавливается равным сроку действия сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа электронной подписи устанавливается Удостоверяющим Центром в момент его изготовления.

Срок действия сертификата ключа подписи пользователя УЦ определяется путем выбора минимального из установленных сроков областей использования

сертификатов, приведенных в Таблице 1, из числа областей использования, указанных в соответствующем заявлении на изготовление сертификата ключа подписи.

Таблица 1. Пример таблицы сроков областей использования сертификатов

№ п/п	Наименование области использования	Объектный идентификатор	Срок
1.	Центр Регистрации	1.2.643.2.2.34.7	1 год
2.	Администратор Центра Регистрации	1.2.643.2.2.34.4	1 год
3.	Оператор Центра Регистрации	1.2.643.2.2.34.5	1 год
4.	Пользователь Центра Регистрации	1.2.643.2.2.34.6	1 год
5.	Временный доступ к Центру Регистрации	1.2.643.2.2.34.2	1 неделя
6.	Защищенная электронная почта	1.3.6.1.5.5.7.3.4	1 год
7.	Проверка подлинности клиента	1.3.6.1.5.5.7.3.2	1 год
8.	Проверка подлинности сервера	1.3.6.1.5.5.7.3.1	1 год

7.10. Архивное хранение документированной информации

7.10.1. Состав архивируемых документов

Архивированию подлежат следующая документированная информация:

- Реестр сертификатов ключей пользователей УЦ;
- сертификаты ключей проверки подписи уполномоченного лица Удостоверяющего Центра;
- журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего Центра;
- Реестр зарегистрированных пользователей Удостоверяющего Центра;
- заявления на изготовление ключей пользователей УЦ;
- заявления на изготовление сертификатов ключей пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов открытых ключей;
- служебные документы Удостоверяющего Центра.

7.10.2. Источник комплектования архивного фонда

Источником комплектования архивного фонда Удостоверяющего Центра являются подразделения (Службы) Удостоверяющего Центра, обеспечивающие документирование.

7.10.3. Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

7.10.4. Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов устанавливается 5 лет для обеспечения возможности в последующем выполнения процедуры разбора конфликтных ситуаций.

7.10.5. Уничтожение архивных документов

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

8. Структуры сертификатов и списков отозванных сертификатов

8.1. Структура квалифицированного сертификата ключа электронной подписи, изготавливаемого Удостоверяющим Центром в электронной форме

Удостоверяющий Центр издает сертификаты открытых ключей пользователей УЦ и уполномоченного лица Удостоверяющего Центра в электронной форме (далее по тексту раздела сертификаты открытых ключей) формата X.509 версии 3.

8.1.1. Базовые поля сертификата ключа подписи

Сертификаты открытых ключей содержат следующие базовые поля X.509:

- Signature: Электронная подпись уполномоченного лица Удостоверяющего Центра;
- Issuer: Идентифицирующие данные уполномоченного лица Удостоверяющего Центра;
- Validity: даты начала и окончания срока действия сертификата;
- Subject: Идентифицирующие данные владельца сертификата ключа подписи;
- SubjectPublicKeyInformation: Идентификатор алгоритма средства электронной подписи, с которыми используется данный ключ, значение ключа подписи;
- Version: версия сертификата формата X.509 - версия 3;
- SerialNumber: уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов открытых ключей Удостоверяющего Центра;
- Signature Algorithm: алгоритм подписи;
- Public Key: открытый ключ.

8.1.2. Дополнения сертификата

Сертификаты открытых ключей содержат следующие дополнения:

- authorityKeyIdentifier идентификатор ключа уполномоченного лица Удостоверяющего Центра;
- subjectKeyIdentifier идентификатор ключа владельца сертификата;
- ExtendedKeyUsage Область (области) использования ключа, при которых электронный документ с электронной подписью будет иметь юридическое значение;
- cRLDistributionPoint точка распространения списка аннулированных (отозванных) сертификатов открытых ключей, изданных Удостоверяющим Центром;
- KeyUsage Назначение ключа;
- Certificate Policies Политики сертификации;
- Authority Information Access Точки распространения сертификата ключа

проверки электронной подписи Уполномоченного лица Удостоверяющего центра;

- SubjectSignTool Наименование средства ЭП, используемое владельцем сертификата;
- IssuerSignTool Наименование средств ЭП и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, а также реквизиты документов, подтверждающих соответствие указанных средств требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

8.1.3. Формы имени

В сертификате ключа электронной подписи поля идентификационных данных уполномоченного лица Удостоверяющего Центра и владельца сертификата содержат атрибуты имени формата X.509.

8.1.4. Ограничения на имена

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего Центра являются:

- Common Name Фамилия, имя, отчество;
- Organization Наименование организации, являющейся владельцем Удостоверяющего Центра;
- Organization Unit Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего Центра;
- Email Адрес электронной почты;
- Country RU;
- State Субъект Федерации, где зарегистрирована организация, являющейся владельцем Удостоверяющего Центра.

Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом, являются:

- Common Name Фамилия, имя, отчество;
- Email Адрес электронной почты;
- Country RU.

Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом и представляющего юридическое лицо, являются:

- Common Name Фамилия, имя, отчество;
- Organization Наименование организации, которую представляет владелец сертификата;
- Organization Unit Наименование подразделения организации, сотрудником которого является владелец сертификата;
- Email Адрес электронной почты;
- Country RU;
- State Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата.

8.1.5. Требования к составу сертификата ключа подписи участника размещения заказа на электронных торговых площадках

Сертификат ключа подписи, издаваемый удостоверяющим центром для участника размещения заказа должен соответствовать стандарту X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 6986 «GOST R

34.11-2012: Hash Func-tion», RFC 7091 «GOST R 34.10- 2012: Digital Signature Algorithm», RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012».

Сертификат ключа подписи участника размещения заказа должен соответствовать следующей структуре:

Название	**Описание**	**Содержание**
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer	Издатель сертификата	CN = Псевдоним уполномоченного лица Удостоверяющего центра O = Организация OU = Подразделение L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта Конкретный перечень компонент имени уполномоченного лица Удоствоеряющего центра устанавливается Удостоверяющим центром по согласованию с Уполномоченным оператором
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CN = ФИО владельца сертификата T = Должность - для юридических лиц 1. O = Наименование организации - для юридических лиц; Наименование ИП – для ИП OU = Подразделение - для юридических лиц L = Город S = Субъект федерации C = Страна/Регион= RU E = Электронная почта 2. UnsructuredName (UN) = INN=ИНН/KPP=КПП/OGRN=ОГРН - для юридических лиц; INN=ИНН - для физических лиц и ИП В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 5280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя	ГОСТ Р 34.11-2012/34.10-2012 256 бит

	сертификата	
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Key Usage	Использование ключа	Информация об использовании ключа. Значение данного поля должно обеспечивать использование ключа для формирования ЭЦП и шифрования данных
Extended Key Usage	Улучшеный ключ	Указываются идентификат оры областей использования закрытых ключей и сертификатов открытых ключей: Проверка подлинности клиента (OID 1.3.6.1.5.5.7.3.2) Защищенная электронная почта (OID 1.3.6.1.5.5.7.3.4) Использование на электронных площадках, отобранных для проведения аукционов в электронной форме (OID 1.2.643.6.3.1.1) Области использования согласно заявлению клиента: Тип участника (один вариант из списка) – Юридическое лицо(OID 1.2.643.6.3.1.2.1) – Физическое лицо(OID 1.2.643.6.3.1.2.2) – Индивидуальный предприниматель(OID 1.2.643.6.3.1.2.3) Тип организации: – Участник размещения заказа(OID 1.2.643.6.3.1.3.1) Полномочия (множественный выбор): – Администратор организации(OID 1.2.643.6.3.1.4.1) – Уполномоченный специалист(OID 1.2.643.6.3.1.4.2) – Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3)
	Политика применения	Набор дополнительных областей использования ключей и сертификатов Устанавливается Удостоверяющим центром по согласованию с Уполномоченным оператором
Certificate Policies	Политики сертификатов	Набор дополнительных областей использования ключей и сертификатов Устанавливается Удостоверяющим центром по согласованию с Уполномоченным оператором
Subject Key Idendifier	Идентификатор ключа владельца	Идентификатор закрытого ключа владельца сертификата

	сертификата	
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, Name - имя файла списка отозванных сертификатов.
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 5280

Поле «Субъект» сертификата ключа подписи, идентифицирующего владельца сертификата ключа подписи, должно содержать следующие компоненты имени:

– компонент «Общее имя» (CN, Common Name), содержащий фамилию, имя, отчество владельца сертификата с разделителями в один пробел (Фамилия Имя Отчество) (обязательное к заполнению);

– компонент «Организация» (O, Organization), содержащий:

- краткое название организации (согласно ЕГРЮЛ) - для юридических лиц (обязательное к заполнению);
- название индивидуального предпринимателя – для индивидуальных предпринимателей (обязательное к заполнению);
- не заполняется – для физических лиц.

– компонент «Должность» (T, Title), содержащий:

- название должности владельца сертификата в организации - для юридических лиц (обязательное к заполнению);
- не заполняется – для индивидуальных предпринимателей и физических лиц.

– компонент «Подразделение» (OU, Organization Unit), содержащий наименование подразделения организации, в котором работает владелец сертификата – для юридических лиц (не обязательное к заполнению);

– компонент «Город» (L, Locality), содержащий название населённого пункта, где зарегистрировано юридическое лицо, индивидуальный предприниматель, физическое лицо (обязательное к заполнению);

компонент «Область/Край» (S, State), содержащий название региона, где зарегистрировано юридическое лицо, индивидуальный предприниматель, физическое лицо (обязательное к заполнению);

– компонент «Страна/регион» (C, Country), содержащее двухзначный код страны (например, «RU»), в которой зарегистрировано юридическое лицо, индивидуальный предприниматель, физическое лицо (обязательное к заполнению);

– компонент «Электронная почта» (E, EMail), содержащее адрес электронной почты владельца сертификата ключа подписи (обязательное к заполнению);

– компонент «Неструктурированное имя» (UN, Unsructured Name), содержащее:

- INN=ИНН/KPP=КПП/OGRN=ОГРН организации владельца сертификата - для юридических лиц (обязательное к заполнению);
- INN=ИНН индивидуального предпринимателя – для индивидуального предпринимателя (обязательное к заполнению);
- INN=ИНН физического лица - для физических лиц (обязательное к заполнению).

В сертификате ключа подписи участника размещения заказа расширение «Улучшенный ключ» (OID 2.5.29.37) должно содержать значения: «Проверка подлинности клиента» (OID 1.3.6.1.5.5.7.3.2), «Защищенная электронная почта» (OID 1.3.6.1.5.5.7.3.4).

В сертификате ключа подписи в расширении «Улучшенный ключ», согласно заявлению участника размещения заказа, содержатся сведения, устанавливающие правомерность использования сертификата ключа подписи на электронных площадках:

- Использование в работе систем электронного документооборота и электронных торговых систем, входящих в АЭТП (1.2.643.6.3);
- Использование в работе систем электронного документооборота и электронных торговых систем B2B-CENTER (OID 1.2.643.6.7);
- Использование на электронных площадках, отобранных для проведения открытых аукционов в электронной форме (OID 1.2.643.6.3.1.1);
- АО «Центр дистанционных торгов» Организатор торгов (продавец) (OID 1.2.643.6.18.1);
- АО «Центр дистанционных торгов» Участник торгов (покупатель) (OID 1.2.643.6.18.2);
- Региональная торговая площадка (OID 1.2.643.6.53);
- Фабрикант (OID 1.2.643.6.15);
- Центр реализации (OID 1.2.643.6.14);
- ГПБ (OID 1.2.643.6.17.1).

Тип участника (один вариант из списка):

- Юридическое лицо (OID 1.2.643.6.3.1.2.1);
- Физическое лицо (OID 1.2.643.6.3.1.2.2);
- Индивидуальный предприниматель (OID 1.2.643.6.3.1.2.3).

Тип организации: Участник размещения заказа (OID 1.2.643.6.3.1.3.1)

Полномочия (множественный выбор):

- Администратор организации (OID 1.2.643.6.3.1.4.1);
- Уполномоченный специалист (OID 1.2.643.6.3.1.4.2);
- Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3).

Список аннулированных сертификатов, издаваемый удостоверяющим центром должен соответствовать стандарту X.509v2 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 6986 «GOST R 34.11-2012: Hash Function», RFC 7091 «GOST R 34.10- 2012: Digital Signature Algorithm», RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012, RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

8.2. Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = Псевдоним уполномоченного лица Удостоверяющего центра O = Организация OU = Подразделение L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта

		Конкретный перечень компонент имени уполномоченного лица Удоствоеряющего центра устанавливается Удостоверяющим центром по согласованию с Уполномоченным оператором
thisUpdate	Время изготовления СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список аннулированных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего центра Устанавливается Удостоверяющим центром по согласованию с Уполномоченным оператором
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС Устанавливается Удостоверяющим центром по согласованию с Уполномоченным оператором
		В список аннулированных сертификатов могут быть добавлены дополнительные поля и расширения согласно RFC 5280

9. Программные и технические средства обеспечения деятельности Удостоверяющего Центра

Для реализации своих услуг и обеспечения жизнедеятельности Удостоверяющий Центр использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра (далее по тексту, ПК УЦ);
- Технические средства обеспечения работы ПК УЦ (далее по тексту, ТС УЦ);
- Программные и программно-аппаратные средства защиты информации (далее по тексту - СЗИ УЦ).

9.1. Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра

Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра включает в себя следующие программные компоненты:

- Центр Сертификации;
- Центр Регистрации;
- АРМ администратора ЦР;
- АРМ разбора конфликтных ситуаций.

Центр Сертификации является базовым серверным компонентом ПК УЦ и предназначен для обеспечения реализации следующих целевых функций Удостоверяющего Центра:

1. Формирования сертификатов открытых ключей пользователей УЦ в электронной форме с использованием закрытого ключа и сертификата ключа подписи уполномоченного лица Удостоверяющего Центра;

2. Формирования списков аннулированных (отозванных) сертификатов пользователей УЦ (СОС) в электронной форме с использованием закрытого ключа и сертификата ключа электронной подписи уполномоченного лица Удостоверяющего Центра на основе эталонной копии списка аннулированных (отозванных) сертификатов открытых ключей пользователей УЦ;

3. Ведения эталонной копии Реестра сертификатов открытых ключей Удостоверяющего Центра;

4. Ведения эталонной копии списка аннулированных (отозванных) сертификатов пользователей УЦ;

5. Обеспечения уникальности открытых ключей в изданных сертификатах открытых ключей пользователей УЦ.

Ответственность за эксплуатацию Центра Сертификации возлагается на уполномоченное лицо Удостоверяющего Центра.

Центр Регистрации является серверным компонентом ПК УЦ и предназначен для обеспечения реализации следующих целевых функций Удостоверяющего Центра:

1. Ведения Реестра зарегистрированных пользователей Удостоверяющего Центра;

2. Ведения Реестра сертификатов открытых ключей Удостоверяющего Центра;

3.Ведения Реестра заявлений на изготовление сертификатов открытых ключей пользователей УЦ в электронной форме;

4. Ведения Реестра заявлений на аннулирование (отзыв) сертификатов открытых ключей пользователей УЦ в электронной форме;

5. Ведения Реестра запросов на регистрацию пользователей УЦ в электронной форме;

6. Предоставления программных средств для:

a. Пользователей УЦ Группы 1 для обеспечения реализации их права передать по сети на Удостоверяющий Центр запрос на регистрацию в электронной форме;

b. Зарегистрированных пользователей УЦ Группы 2 и 3 для обеспечения реализации их прав в части пользования предоставляемыми программными средствами;

Ответственность за эксплуатацию Центра Регистрации возлагается на Службу Регистрации УЦ.

АРМ администратора ЦР является приложением ПК УЦ и предназначен для обеспечения реализации своих функциональных обязанностей сотрудникам Службы Регистрации и Службы Безопасности УЦ.

АРМ разбора конфликтных ситуаций является приложением ПК УЦ и предназначен для

обеспечения своих функциональных обязанностей сотрудникам Административной Службы УЦ в части взаимодействия с пользователями УЦ при разрешении вопросов, связанных с подтверждением электронной подписи уполномоченного лица Удостоверяющего Центра в сертификатах открытых ключей, изготовленных Удостоверяющим Центром в электронной форме.

9.2. Технические средства обеспечения работы ПК УЦ

Технические средства обеспечения работы ПК УЦ включают в себя:

- Выделенный сервер Центра Сертификации;
- Выделенный сервер Центра Регистрации;
- Телекоммуникационное оборудование;
- Компьютеры рабочих мест сотрудников Служб Удостоверяющего Центра;
- Устройства печати на бумажных носителях (принтеры).

Ответственность за эксплуатацию технических средств и общесистемного программного обеспечения возлагается на Техническую Службу УЦ.

9.3. Программные и программно-аппаратные средства защиты информации

Программные и программно-аппаратные средства защиты информации включают в себя:

- Средства криптографической защиты информации;
- Межсетевой экран для обеспечения защиты информации при сетевом взаимодействии с Центром Регистрации;
- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Устройства обеспечения бесперебойного питания серверов Центра Сертификации и Центра Регистрации;
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений Удостоверяющего Центра;
- Устройства обеспечения противопожарной безопасности помещений Удостоверяющего Центра.

Средства криптографической защиты информации, эксплуатируемые на всех компонентах ПК УЦ, сертифицированы по классу «КС2» в соответствии с действующим законодательством Российской Федерации.

Ответственность за эксплуатацию программных и программно-аппаратных средств защиты информации возлагается на Техническую Службу УЦ.

9.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций Удостоверяющего Центра

- Центром Сертификации:
  - Установлено сетевое соединение с программной компонентой Центра Регистрации;
  - Издан СОС;
  - Принят запрос на сертификат ключа подписи;
  - Издание сертификата ключа подписи;
  - Невыполнение внутренней операции программной компоненты;
  - Системные события общесистемного программного обеспечения.
- Центром Регистрации:
  - Помещен запрос на регистрацию;
  - Принят запрос на регистрацию;
  - Отклонен запрос на регистрацию;
  - Помещен запрос на сертификат;

- Принят запрос на сертификат;
- Отклонен запрос на сертификат;
- Установка сертификата подтверждена пользователем;
- Помещен запрос на отзыв сертификата;
- Принят запрос на отзыв сертификата;
- Отклонен запрос на отзыв сертификата;
- Помещен запрос на первый сертификат;
- Запрошен список аннулированных сертификатов;
- Опубликован список аннулированных сертификатов;
- Невыполнение внутренней операции программной компоненты;
- Установлено сетевое соединение с внешней программной компонентой;
- Системные события общесистемного программного обеспечения.

Структуры записей событий приведены в эксплуатационной документации программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра и общесистемного программного обеспечения.

9.5. Перечень данных программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра, подлежащих резервному копированию.

При эксплуатации программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра ежесуточно выполняется резервное копирование данных компонент ПК УЦ.

Перечень данных ПК УЦ, подлежащих резервному копированию, включает в себя:

- Сертификат ключа электронной подписи уполномоченного лица Удостоверяющего Центра в электронном виде (сертификат службы сертификации Центра Сертификации ПК УЦ);
- Базу данных службы сертификации Центра Сертификации ПК УЦ, включая журнал выданных сертификатов и очередь запросов;
- Базу данных Центра Регистрации ПК УЦ (базу данных SQL сервера Центра Регистрации);
- Журналы аудита компонент ПК УЦ в составе, определенной эксплуатационной документацией ПК УЦ.

10. Обеспечение безопасности

10.1. Инженерно-технические меры защиты информации

10.1.1. Размещение технических средств Удостоверяющего Центра

Сервера Центра Сертификации, Центра Регистрации, АРМ администратора и АРМ Разбора конфликтных ситуации, а также телекоммуникационное оборудование размещены в выделенном помещении.

Сервера Центра Сертификации, Центра Регистрации и телекоммуникационное оборудование размещаются в шкафу-стойке.

10.1.2. Физический доступ в помещения

Серверное помещение Удостоверяющего Центра оборудовано кодовым замком.

Рабочие и служебные помещения Удостоверяющего Центра не подключены к системе контроля доступа и оборудованы механическими замками

Порядок доступа в серверное помещение определен в приказе руководителя УЦ.

10.1.3. Электроснабжение и кондиционирование воздуха

Технические средства Удостоверяющего Центра подключены к общегородской сети

электроснабжения.

Сервера Центра Сертификации и Центра Регистрации, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течении 4 часов после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников Удостоверяющего Центра, источниками бесперебойного питания не оборудуются.

Рабочие и прочие служебные помещения Удостоверяющего Центра оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

10.1.4. Предупреждение и защита от возгорания

Серверное помещение Удостоверяющего Центра оборудовано системой пожарной сигнализации.

10.1.5. Хранение документированной информации

Документальный фонд Удостоверяющего Центра, как фондообразователя, подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

10.1.6. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками Удостоверяющего Центра, обеспечивающих документирование.

10.2. Программно-аппаратные меры защиты информации

10.2.1. Организация доступа к техническим средствам Удостоверяющего Центра

Доступ к техническим средствам Удостоверяющего Центра, размещенным в выделенном помещении, осуществляется на основании приказа руководителя организации.

10.2.2. Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого Удостоверяющим Центром:

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Центра Сертификации;
- Программные модули Центра Регистрации.

Система контроля целостности программных модулей, подлежащих контролю целостности, основывается на аппаратном контроле целостности и общесистемного программного обеспечения до загрузки операционной системы.

Данная система контроля целостности обеспечивается использованием сертифицированного устройства типа «электронный замок».

Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется с использованием средств электронной подписи и криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности - ежесуточно.

Ответственность за выполнение мероприятий по контролю целостности программных средств возложена на Службу Безопасности УЦ.

10.2.3. Контроль целостности технических средств

Контроль целостности технических средств технических средств Удостоверяющего Центра

обеспечивается опечатыванием корпусов устройств, препятствующих их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию, и после выполнения регламентных работ.

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

Ответственность за выполнение мероприятий по контролю целостности технических средств возложена на Службу Безопасности УЦ.

10.2.4. Организация доступа к программным средствам Удостоверяющего Центра

Сервера Центра Сертификации и Центра Регистрации оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа.

Рабочие места сотрудников Удостоверяющего Центра, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» также оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа.

10.2.5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности Удостоверяющего Центра и программными средствами, предоставляемыми Удостоверяющим Центром пользователям УЦ, в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации.

В качестве шифровальных (криптографических) средств пользователей УЦ, используемых для защиты конфиденциальной информации, используется средство электронной подписи пользователя УЦ.

Защита программно-технических средств обеспечения деятельности Удостоверяющего Центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана не ниже 4-го класса защиты.

10.2.6. Перечень информации, подлежащей защите

Поступающая в Удостоверяющий Центр информация:

- Заявление на регистрацию в электронной форме;
- Заявление на изготовление сертификата ключа электронной подписи в электронной форме;
- Заявление на аннулирование (отзыв) сертификата ключа электронной подписи в электронной форме;
- Пароль, передаваемый пользователем УЦ при аутентификации по паролю;
- Ключевая фраза пользователя УЦ.

Передаваемая из Удостоверяющего Центра информация:

- Пароль, передаваемый пользователю УЦ для аутентификации по паролю;
- Бланк копии сертификата ключа электронной подписи для вывода на бумажный носитель;
- Список сертификатов ключа подписи пользователя УЦ и их статус;
- Список запросов на сертификаты открытых ключей пользователя УЦ и их статус;
- Список запросов на аннулирование (отзыв) сертификатов пользователя УЦ и их статус.

10.3. Организационные меры защиты информации

10.3.1. Предъявляемые требования к персоналу Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет.

Сотрудники Службы Безопасности УЦ имеют высшее профессиональное образование и прошли курсы повышение квалификации в области информационной безопасности с получением специализации в области систем с открытым распределением ключей.

10.3.2. Профессиональная переподготовка и повышение квалификации персонала

Профессиональная переподготовка персонала Удостоверяющего Центра не осуществляется.

Сотрудники Удостоверяющего Центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

10.3.3. Организация доступа персонала к документам и документации

Доступ сотрудников Удостоверяющего Центра к документам и документации, составляющей документальный фонд организации, организован в соответствии с функциональными обязанностями.

10.3.4. Охрана здания и помещений

Удостоверяющий Центр имеет привлекаемую службу охраны здания и помещений, обеспечивающую:

- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) Удостоверяющего Центра;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

10.4. Юридические меры защиты информации

Удостоверяющий Центр имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг (см. п.2.1).

Системы безопасности Удостоверяющего Центра и защиты информации созданы и поддерживаются на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством Российской Федерации.

Все меры по защите информации на Удостоверяющем Центре введены в действие приказами руководителя Удостоверяющего Центра.

Для обеспечения деятельности Удостоверяющий Центр использует средства электронной подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы Удостоверяющего Центра находятся в собственности Удостоверяющего Центра.

Пользователям УЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые Удостоверяющим Центром.

Приложение №1 к Регламенту

Заявление на изготовление квалифицированного сертификата ключа подписи для юридических лиц

МОСТ ИНФО

Директору
ООО "МОСТИНФО"
Вилисовой Ирине Борисовне
От _____
(должность руководителя)
_____
(название организации)
_____
(ФИО руководителя)

Заявление на изготовление сертификата ключа проверки электронной подписи и присоединение к Регламенту Удостоверяющего центра ООО "МОСТИНФО"

Прошу сформировать ключи и изготовить сертификат ключа подписи (СКП) для уполномоченного сотрудника организации, в соответствии с указанными в настоящем заявлении данными:

Краткое наименование организации (ЮЛ):						
ФИО (владельца СКП):						
Должность (владельца СКП):						
Юридический адрес:						
Контактный телефон:	+ 7 ( )					
Адрес электронной почты:						
Паспортные данные (владельца СКП):	Серия		№		Дата выдачи	
Кем выдан:						
Зарегистрирован:						
СНИЛС (владельца СКП):						
ИНН/КПП/ОГРН:						
Встроенная лицензия крипто-про:						
Область применения сертификата (OID)						

Ознакомлен с требованиями Регламента Удостоверяющего центра ООО «МОСТИНФО» и приложениями к нему, в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.
В целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО "МОСТИНФО", формирования общедоступных справочников сертификатов ключей подписей, списков отозванных сертификатов ключей подписей, исполнения требований Федеральных Законов от 06.04.2011 № 63-ФЗ "Об электронной подписи", от 27.07.2006 № 152-ФЗ "О персональных данных" своей волей и в своем интересе даю согласие ООО «МОСТИНФО», расположенному по адресу: 620075, Свердловская обл., г. Екатеринбург, ул. Первомайская, д. 15, оф. 1204, на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение, передачу, распространение) с использованием средств автоматизации или без использования таких моих персональных данных:
- фамилия, имя, отчество, место работы (наименование организации), должность, телефон, адрес электронной почты, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), адрес работы и места жительства, в целях исполнения договорных отношений (при условии соблюдения конфиденциальности) и иные сведения, необходимые для исполнения целей Регламента удостоверяющего центра, на хранение скан копий документа, удостоверяющего личность, СНИЛС. Признаю, что мои персональные данные, которые будут занесены в сертификаты ключей проверки электронных подписей, будут отнесены к общедоступным персональным данным в соответствии с п.3 ст.15 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи". Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации установленного п.2 ст.15 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи" и может быть отозвано мною в любое время на основании моего письменного заявления. В случае отзыва согласия на обработку моих персональных данных признаю, что Удостоверяющий центр ООО "МОСТИНФО" вправе не прекращать их обработку до окончания срока действия настоящего согласия, при прекращении обработки моих персональных данных прошу меня об этом не уведомлять.

Владелец (СКП): _____ (должность) / _____ (ФИО владельца СКП) / _____ Личная подпись владельца СКП

Руководитель организации:

Сведения о сотруднике представлены на основании подлинных документов, перечень которых указан в Регламенте, и являются достоверными.

_____ (должность) / _____ (ФИО руководителя) / _____ Личная подпись руководителя

М.П.

Дата заполнения заявки

Ответственный за идентификацию

_____ (должность) / _____ (ФИО) / _____ Личная подпись

Приложение №2 к Регламенту

Заявление на изготовление квалифицированного сертификата ключа подписи для физических лиц

Директору
ООО "МОСТИНФО"
Вилисовой Ирине Борисовне
От физического лица

(ФИО)

Заявление на изготовление сертификата ключа проверки электронной подписи и присоединение к Регламенту Удостоверяющего центра ООО "МОСТИНФО"

Прошу сформировать ключи и изготовить сертификат ключа подписи (СКП) для физического лица с целью _____ в соответствии с указанными в настоящем заявлении данными:
(указать для каких целей нужна ЭП)

ФИО (владельца СКП):						
Контактный телефон:						
Адрес электронной почты:						
СНИЛС (владельца СКП):						
Паспортные данные (владельца СКП):	Серия		№		Дата выдачи	
Кем выдан:						
Зарегистрирован:						
ИНН(владельца СКП):						
Встроенная лицензия крипто-про:						
Область применения сертификата (OID)						

Ознакомлен с требованиями Регламента Удостоверяющего центра ООО «МОСТИНФО» и приложениями к нему, в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.
В целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО "МОСТИНФО", формирования общедоступных справочников сертификатов
ключей подписей, списков отозванных сертификатов ключей подписей, исполнения требований Федеральных Законов от 06.04.2011 № 63-ФЗ "Об электронной подписи", от 27.07.2006 № 152-ФЗ "О персональных данных" своей волей и в своем интересе даю согласие ООО «МОСТИНФО», расположенному по адресу: 620075, Свердловская обл., г. Екатеринбург, ул. Первомайская, д. 15, оф. 1204, на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование,
обезличивание, блокирование, уничтожение, передачу, распространение) с использованием средств автоматизации или без использования таких моих персональных данных:
фамилия, имя, отчество, место работы (наименование организации), должность, телефон, адрес электронной почты, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), адрес работы и места жительства, в целях исполнения договорных отношений (при условии соблюдения конфиденциальности) и иные сведения, необходимые для исполнения целей Регламента удостоверяющего центра, на хранение скан копий документа, удостоверяющего личность, СНИЛС. Признаю, что мои персональные данные, которые будут занесены в сертификаты ключей проверки электронных подписей, будут отнесены к общедоступным персональным данным в соответствии с п.3 ст.15 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи". Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации установленного п.2 ст.15 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи" и может быть отозвано мною в любое время на основании моего письменного заявления. В случае отзыва согласия на обработку моих персональных данных признаю,что Удостоверяющий центр ООО "МОСТИНФО" вправе не прекращать их обработку до окончания срока действия настоящего согласия, при прекращении обработки моих персональных данных прошу меня об этом не уведомлять.

Владелец (СКП): физическое лицо _____ / _____
(ФИО владельца СКП) Личная подпись владельца СКП

Дата заполнения заявки

Ответственный за идентификацию

_____ / _____ / _____
(должность) (ФИО) Личная подпись

Приложение №3 к Регламенту

Заявление на изготовление квалифицированного сертификата ключа подписи для индивидуальных предпринимателей

Директору
ООО "МОСТИНФО"
Вилисовой Ирине Борисовне
От Индивидуального предпринимателя
(должность руководителя)
ИП
(ФИО ИП в именительном падеже)
(ФИО предпринимателя в родительном падеже)

Заявление на изготовление сертификата ключа проверки электронной подписи и присоединение к Регламенту Удостоверяющего центра ООО "МОСТИНФО"

Прошу сформировать ключи и изготовить сертификат ключа подписи (СКП) для уполномоченного сотрудника организации, в соответствии с указанными в настоящем заявлении данными:

ИП ФИО (владельца СКП):	ИП					
ФИО (владельца СКП):						
Юридический адрес:						
Контактный телефон:	+ 7 ( )					
Адрес электронной почты:						
Паспортные данные (владельца СКП):	Серия		№		Дата выдачи	
Кем выдан:						
Зарегистрирован:						
СНИЛС (владельца СКП):						
ИНН/ОГРНИП:						
Встроенная лицензия крипто-про:						
Область применения сертификата (OID)						

Ознакомлен с требованиями Регламента Удостоверяющего центра ООО «МОСТИНФО» и приложениями к нему, в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.
В целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО "МОСТИНФО", формирования общедоступных справочников сертификатов ключей подписей, списков отозванных сертификатов ключей подписей, исполнения требований Федеральных Законов от 06.04.2011 № 63-ФЗ "Об электронной подписи", от 27.07.2006 № 152-ФЗ "О персональных данных" своей волей и в своем интересе даю согласие ООО «МОСТИНФО», расположенному по адресу: 620075, Свердловская обл., г. Екатеринбург, ул. Первомайская, д. 15, оф. 1204, на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение, передачу, распространение) с использованием средств автоматизации или без использования таких моих персональных данных: фамилия, имя, отчество, место работы (наименование организации), должность, телефон, адрес электронной почты, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), адрес работы и места жительства, в целях исполнения договорных отношений (при условии соблюдения конфиденциальности) и иные сведения, необходимые для исполнения целей Регламента удостоверяющего центра, на хранение скан копий документа, удостоверяющего личность, СНИЛС. Признаю, что мои персональные данные, которые будут занесены в сертификаты ключей проверки электронных подписей, будут отнесены к общедоступным персональным данным в соответствии с п.3 ст.15 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи". Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации установленного п.2 ст.15 Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи" и может быть отозвано мною в любое время на основании моего письменного заявления. В случае отзыва согласия на обработку моих персональных данных признаю, что Удостоверяющий центр ООО "МОСТИНФО" вправе не прекращать их обработку до окончания срока действия настоящего согласия, при прекращении обработки моих персональных данных прошу меня об этом не уведомлять.

Владелец (СКП): Индивидуальный предприниматель / _____ / _____
(ФИО владельца СКП) Личная подпись владельца СКП

Руководитель организации:

Сведения о сотруднике представлены на основании подлинных документов, перечень которых указан в Регламенте, и являются достоверными.

Индивидуальный предприниматель / _____ / _____
(ФИО предпринимателя) Подпись предпринимателя

М.П.

Дата заполнения заявки

Ответственный за идентификацию

_____ / _____ / _____
(должность) (ФИО) Личная подпись

Приложение №4 к Регламенту

Форма доверенности на получение ЭП

Доверенность

Дата выдачи доверенности "___" _____ 20___года

Я, _____
(ФИО руководителя)

_____ _____
(должность) (название организации руководителя)

Паспорт РФ _____ _____
(вид документа, удостоверяющего личность) (серия) (номер)

_____
(кем выдан документ)

Дата выдачи документа "___" _____ 20___года

Доверяю _____
(ФИО доверяемого)

_____ _____
(должность) (название организации руководителя)

Паспорт РФ _____ _____
(вид документа, удостоверяющего личность) (серия) (номер)

_____
(кем выдан документ)

Дата выдачи документа "___" _____ 20___года

ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:
вместо меня присутствовать при создании ключей моей электронной подписи (ЭП) и сертификата ключа подписи;
получить ключевой носитель, содержащий:
• ключевые файлы в контейнере;
• сертификат ключа подписи;
• защищенный носитель;
получить мой сертификат ключа подписи;
расписаться за меня в Сертификате ключа подписи, актах;
получить лицензии на право использования программ криптозащиты;
подписать за меня финансовые документы (в рамках выполненных работ и оказанных услуг) и договор.

Доверенность действительна до "___" _____ 20____года

Подпись лица:

_____/_____/_____
(должность) (ФИО) Личная подпись доверенного лица

_____/_____/_____
(должность) (ФИО руководителя) Личная подпись руководителя

Удостоверяю

Руководитель организации:

_____/_____/_____
(должность) (ФИО руководителя) Личная подпись руководителя

М.П.

Приложение №5 к Регламенту

Форма заявления на прекращение действия Сертификата

ЗАЯВЛЕНИЕ НА ОТЗЫВ (ПРИОСТАНОВЛЕНИЕ) СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

г. Екатеринбург **«___» _____ 20__ года**

Я, _____

_____

_____,

(*Ф.И.О., паспортные данные, место жительства)*

Данные сертификата:

Серийный номер сертификата(S\N)=_____

КПП организации =_____

Фамилия Имя Отчество(CN - Общее имя)=_____

Организация (O)=_____

Электронная почта (E)=_____

ИНН (INN)=_____

в связи с _____

_____

(причина отзыва (приостановления) сертификата ключа подписи: компрометация закрытого ключа, прекращение работы и т.д)

прошу отозвать или приостановить сертификат ключа подписи

Нужное подчеркнуть

_____ _____

(фамилия, инициалы) М.П. *(подпись)*

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключа подписи на имя

_____ получено,

(Ф.И.О.)

личность _____

(фамилия, инициалы)

идентифицирована, сведения, указанные в Заявлении проверены.

Директор

ООО «Мостинфо» _____ И. Б. Вилисова

«__» _____ 201__г.