«УТВЕРЖДАЮ»
Директор ООО «МОСТИНФО»

_____/ И.Б. Вилисова

16 марта 2013 г.

Редакция от 06.02.2017 г.

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

Екатеринбург
2017

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: 5.1.

Дата: 06.02.2017 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**.

1.6. Контактная информация

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

Почтовый адрес: 620075, г. Екатеринбург, ул. Первомайская, д.15, оф. 1204

Адрес электронной почты: info@most-info.ru

Телефон (факс): (343) 287-04-67 (365-86-15)

Контактный телефон Технической Службы УЦ: (343) 287-04-67 (доб. 207).

2. Общие положения

2.1. 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.

2.2. Услуги, предоставляемые Удостоверяющим Центром

Удостоверяющий Центр осуществляет свою деятельность на возмездной основе.

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

- создает квалифицированные сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (Пользователям);
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению Пользователя 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 Пользователем;
- 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 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 Пользователей 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.

2.3. 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.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.

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.

Удостоверяющий Центр обязан использовать ключ ЭП уполномоченного лица Удостоверяющего Центра только для подписи издаваемых им сертификатов

ключей ЭП и списков отозванных сертификатов.

Удостоверяющий Центр обязан 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.

Удостоверяющий Центр обязан 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.

Удостоверяющий Центр обязан обеспечить сохранение в тайне изготовленного ключа ЭП.

Удостоверяющий Центр обязан записать ключ на отчуждаемый носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

Удостоверяющий Центр обязан 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.

Удостоверяющий Центр обязан 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.

Удостоверяющий Центр обязан обеспечить уникальность значений ключей ЭП в изготовленных сертификатах ключей пользователей УЦ.

4.1.6. Аннулирование (отзыв) сертификатов ключей ЭП

Удостоверяющий Центр обязан аннулировать (отозвать) сертификат ключа по заявлению его владельца.

Удостоверяющий Центр обязан 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.

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 репозитарии 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 репозитарии Владельца УЦ.

Удостоверяющий Центр обязан включать полный адрес (URL) списка аннулированных сертификатов из репозитария Удостоверяющего Центра в издаваемые сертификаты открытых ключей пользователей УЦ.

4.1.8. Реестр сертификатов ключей

Удостоверяющий Центр обязан вести реестр всех изготовленных сертификатов ключей пользователей УЦ в течение установленного срока хранения.

Реестр сертификатов ключей ведется в электронном виде.

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

Удостоверяющий Центр обязан осуществлять выдачу копий сертификатов ключей в электронной форме по обращениям пользователей УЦ.

Удостоверяющий Центр обязан публиковать выписки из реестра, позволяющие определить действительность сертификатов ключей пользователей УЦ.

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

4.1.9. Прочие обязательства

Удостоверяющий Центр обязан уведомлять владельца сертификата ключа о фактах, которые стали известны Удостоверяющему Центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа.

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;
- 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;
- 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.

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 так же 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 регистрации пользователей УЦ

Удостоверяющий центр осуществляет регистрацию пользователей УЦ только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с пунктом 2.8. настоящего Регламента.

Под регистрацией пользователей УЦ понимается внесение регистрационной информации о пользователях УЦ в реестр Удостоверяющего Центра.

Процедура регистрации пользователей УЦ применяется в отношении физических лиц или юридических лиц, обращающихся к услугам Удостоверяющего Центра в части изготовления сертификатов ключей пользователей УЦ и/или формирования ключей электронной подписи и ключей проверки электронной подписи пользователей УЦ с записью их на ключевой носитель.

6.1.1. Заявление на регистрацию

Сторона, присоединившаяся к настоящему регламенту, предоставляет в Удостоверяющий центр следующие сведения и копии документов, их подтверждающие:

- Для физического лица:
  - Идентификационные данные, включающие:
    - Фамилию, имя и отчество;
    - Адрес электронной почты.
  - Паспортные данные (или другого документа, удостоверяющего личность)
    - Вид документа;
    - Серия документа;
    - Номер документа;

        - Кем выдан;
        - Когда выдан.
    - ИНН
    - Контактные телефоны
    - Страховой номер индивидуального лицевого счета
    - Фотографию в анфас совместно с разворотом 2-3 страницы паспорта.
- Для юридического лица:
    - Идентификационные данные, включающие:
        - Фамилию, имя и отчество уполномоченного представителя;
        - Адрес электронной почты;
        - Наименование юридического лица;
        - Субъект Федерации, в котором зарегистрирована организация;
        - Должность уполномоченного представителя.
    - ИНН юридического лица
    - ОГРН юридического лица
    - Адрес юридического лица
    - СНИЛС уполномоченного представителя
    - Данные доверенности (или других документов, подтверждающих правомочность действий от имени юридического лица)
    - Фотографию уполномоченного представителя в анфас совместно с разворотом 2-3 страницы паспорта;

Дополнительно (определяется заявителем) заявление может содержать следующую информацию, включаемую в идентификационные данные:

- Псевдоним;
- Почтовый и/или юридический адрес.

Заявитель обязан предоставить цветные скан-копии оригиналов документов курирующему менеджеру или принести документы в бумажном виде лично в офис удостоверяющего центра.

К заявлению лица, действующего в интересах юридического лица, прилагаются оригинал доверенности или копии документов, подтверждающих правомочность действий от имени юридического лица.

6.1.2. Идентификация пользователя УЦ

Идентификатором зарегистрированного пользователя являются идентификационные данные из заявления на регистрацию (см. раздел 6.1.1 настоящего Регламента).

Идентификация пользователя выполняется в процессе его регистрации в качестве зарегистрированного пользователя УЦ.

6.1.3. Регистрация пользователя УЦ в централизованном режиме

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.

Изготовление ключей подписи зарегистрированного пользователя УЦ осуществляется либо зарегистрированным пользователем УЦ самостоятельно, либо сотрудником Службы Регистрации. В последнем случае зарегистрированный пользователь УЦ должен выдать сотруднику Службы Регистрации доверенность на изготовление его ключей подписи. Форма доверенности приведена в Приложении № 3 к Регламенту.

Изготовление ключей подписи производится при помощи специализированных программных средств, предоставляемых УЦ. 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.

6.1.4. Регистрация пользователя УЦ в распределенном режиме

Регистрация пользователя УЦ в распределенном режиме не осуществляется.

6.2. Идентификация зарегистрированного пользователя

Идентификация зарегистрированного пользователя УЦ осуществляется по идентификатору зарегистрированного пользователя, занесенному в реестр Удостоверяющего Центра.

6.3. Изготовление ключей

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

6.3.1. Заявление на изготовление ключей

Заявление на изготовление квалифицированного сертификата ключа подписи подается заявителем в простой письменной форме на бумажном носителе и заверяется собственноручной подписью заявителя. 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 подписи рассматривается Службой Безопасности УЦ в течение одного рабочего дня с момента поступления.

6.3.2. Изготовление и выдача ключей владельцу

Изготовление ключей выполняется ответственным сотрудником Службы Безопасности УЦ на специализированном рабочем месте, на основании принятого заявления в присутствии заявителя.

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). Факт выдачи ключей заносится в Журнал учета изготовления и выдачи ключей под роспись владельца.

6.4. Изготовление сертификата ключа проверки электронной подписи и предоставление его владельцу

Изготовление сертификата ключа проверки электронной подписи

осуществляется Удостоверяющим Центром на основании заявления на изготовление сертификата ключа зарегистрированного пользователя УЦ.

Заявление на изготовление сертификата ключа подается заявителем в электронной или бумажной форме в Службу 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.

Изготовленный сертификат ключа в электронной форме, заверенный электронной подписью уполномоченного лица Удостоверяющего Центра, предоставляется его владельцу путем отправки с официальным уведомлением в виде прикрепленного файла, содержащий изготовленный сертификат в электронной форме.

Копия сертификата ключа на бумажном носителе предоставляется его владельцу при личном обращении или его уполномоченного представителя, действующего на основании доверенности, в Службу Безопасности УЦ.

6.4.1. Заявление на изготовление сертификата ключа в электронной форме

Заявление на изготовление сертификата ключа в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве подписываемых данных запрос на сертификат в формате PKCS#10 и подписанный электронной подписью с использованием ключа подписи и сертификата ключа, владельцем которых заявитель является.

В качестве ключа подписи должен использоваться ключ, до окончания срока действия, которого, на момент поступления заявления в Службу Безопасности УЦ, остается не менее 1 календарного месяца.

6.4.2. Заявление на изготовление сертификата ключа в бумажной форме

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

Заявление включает в себя следующие обязательные реквизиты:

- Фамилию, имя, отчество заявителя;
- Дата и подпись заявителя;
- Текст запроса на сертификат в формате PKCS#10 в кодировке Base64

Обязательным приложением к заявлению на изготовление сертификата ключа подписи в бумажной форме является файл, содержащий запрос на сертификат в формате PKCS#10 в кодировке Base64, размещенный на носителе.

6.4.3. Идентификация владельца сертификата ключа подписи

Владелец сертификата ключа подписи идентифицируется по значениям атрибутов поля Subject сертификата ключа подписи (см. раздел 8.1 настоящего Регламента).

6.5. Аннулирование (отзыв) сертификата ключа

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.

Срок рассмотрения заявления на отзыв сертификата ключа составляет 30 минут с момента получения заявления владельца сертификата Службой Безопасности УЦ.

После аннулирования (отзыва) сертификата ключа электронной подписи его владельцу направляется официальное уведомление (см. раздел 4.1.10 настоящего Регламента).

6.5.1. 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.

6.6. Срок хранения сертификата ключа подписи

Хранение сертификата ключа подписи пользователей УЦ в Реестре сертификатов открытых ключей Удостоверяющим Центром, осуществляется в течении установленного срока действия сертификата ключа подписи.

Срок архивного хранения сертификата ключа электронной подписи устанавливается в соответствии со сроком, определенным разделом 7.5 настоящего Регламента.

6.7. Уничтожение ключей

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 ПО СКЗИ «Крипто-Про CSP». Допускается данные носители после переформатирования использовать в дальнейшем Пользователями УЦ при условии записи на них новой ключевой информации.

Выведенные из действия ключи проверки ЭП сохраняются в архивах в течение 5 лет для обеспечения возможности в последующем выполнения процедуры разбора конфликтных ситуаций.

6.8. Процедура подтверждения электронной подписи с использованием сертификата ключа подписи

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.

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

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.

6.9. 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.

6.10. 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. Дополнительные положения

7.1. Сроки действия ключей уполномоченного лица Удостоверяющего Центра

Срок действия ключа электронной подписи уполномоченного лица Удостоверяющего Центра составляет 5 лет.

Начало периода действия ключа уполномоченного лица Удостоверяющего Центра исчисляется с даты и времени начала действия соответствующего сертификата ключа подписи.

Срок действия сертификата ключа электронной подписи, соответствующего ключу уполномоченного лица Удостоверяющего Центра составляет 5 лет.

7.2. Требования к средствам электронной подписи пользователей УЦ

Средство электронной подписи должно обеспечивать 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 7.6).

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).

Идентификаторы алгоритмов должны быть зарегистрированы в настоящем Регламенте в разделе 8.1.3.

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. 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 Таблица 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

7.4. Меры защиты ключей электронной подписи

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.

7.5. Архивное хранение документированной информации

7.5.1. 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.

7.5.2. Источник комплектования архивного фонда

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

7.5.3. Архивохранилище

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

7.5.4. 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.

7.5.5. 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.

7.6. Смена ключей уполномоченного лица Удостоверяющего Центра

7.6.1. Плановая смена ключей уполномоченного лица Удостоверяющего Центра

Плановая смена ключей (закрытого и соответствующего ему ключа электронной подписи) уполномоченного лица Удостоверяющего Центра производится за два месяца до окончания срока действия закрытого ключа уполномоченного лица Удостоверяющего Центра.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего Центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего Центра формирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового ключа подписи и подписывает его электронной подписью с использованием нового ключа электронной подписи.

Старый ключ электронной подписи уполномоченного лица Удостоверяющего Центра используется в течение 1 года с момента изготовления сертификата нового ключа подписи уполномоченного лица Удостоверяющего Центра для формирования списков отозванных сертификатов в электронной форме, изданных Удостоверяющим Центром в период действия старого ключа электронной подписи уполномоченного лица Удостоверяющего Центра.

7.6.2. Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра

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

Процедура внеплановая смена ключей уполномоченного лица Удостоверяющего Центра выполняется в порядке, определенной процедурой плановой смене ключей уполномоченного лица Удостоверяющего Центра.

После выполнения процедуры внеплановой смены ключей уполномоченного лица Удостоверяющего Центра, сертификат ключа электронной подписи уполномоченного лица Удостоверяющего Центра аннулируется (отзывается) путем занесения в список аннулированных сертификатов.

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 сертфиката 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 63-ФЗ

8.1.3. Объектные идентификаторы алгоритма

Удостоверяющий Центр использует следующие идентификаторы алгоритмов средства электронной подписи:

ГОСТ Р 34.10-94 1.2.643.2.2.20
Диффи-Хеллмана 1.2.643.2.2.99
ГОСТ Р 34.10-2001 1.2.643.2.2.19
Диффи-Хеллмана 1.2.643.2.2.98
ГОСТ Р 34.11-94 1.2.643.2.2.9
ГОСТ 28147-89 1.2.643.2.2.21

8.1.4. Формы имени

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

8.1.5. 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

8.1.6. Требования к сертификату ключа подписи и списку отозванных сертификатов для обеспечения единого пространства доверия сертификатам ключей электронной подписи в соответствии с Приказом ФНС №ММ-7-6/353@ от 02.07.09г.

1.2.643.3.<Координирующая организация>.<Эмитент1>. <эмитент2>.<Роль владельца СКП в информационных системах ФНС России (НП, НО, уполномоченный представитель НП, СпецОператор и т.д.)>.<Квалификация подписи (директор, бухгалтер, инспектор НО и т.д.)>.< Пользователь сервисов системы >.<Другие назначения1>.<другие назначения2>

№ арки
1.– 4. зафиксировано **1.2.643.3**
5. **Координирующая организация** – ФНС или Организатор Сети ДУЦ
6. **Эмитент1** – ДУЦ. Содержит идентификатор ДУЦ, формируемый, как 1000+№паспорта ДУЦ. УЦ ГНИВЦ ФНС России имеет идентификатор 1000.
7. **Эмитент2** – УЦ, подчиненный ДУЦ
8. **Роль владельца СКП** в информационных системах ФНС – НП, инспектор НО, уполномоченный представитель НП, ИРУЦ, СОЭД, САОЭД, СпецОператор и т.д.
9. **Квалификация подписи** – 1-я подпись (директор, заместитель директора и т.д.), 2-я подпись (главный бухгалтер, бухгалтер и т.д.), 1-я и 2-я подпись, право подписи отсутствует - только шифровать и/или отправка, квалификация подписи не установлена и т.д.
10. **Пользователь сервисов системы** – сервис ИОН on-line (да или нет), др. сервисы
11. **Другие назначения1** – зарезервировано
12. **Другие назначения2** – зарезервировано

Если в арке №6 стоит число меньше 1000, то эта арка – управляющая, она содержит назначение данных, которые размещены в следующей арке (№7), если в арке №7 число меньше 1000, то арка – управляющая и содержит тип данных, которые размещены в следующей арке (№8) и т.д. В случае с управляющими арками приведённая в начале приложения схема OID применяться не может.

Если арка №6 содержит единицу, то арка – управляющая, указывает на то, что в следующей арке будет указан OID поля сертификата ключа подписи.

Поля сертификата ключа подписи

1.2.643.3.131.1.1 – INN (ИНН)

Объектные идентификаторы политики сертификата

Координирующая организация

1.2.643.3.131 – ГНИВЦ

Эмитент1

1.2.643.3.131.1059 — ООО Мостинфо-Екатеринбург

Эмитент2

1.2.643.3.131.1059.0 — нет

Роль владельца СКП

1.2.643.3.131.1000.0.1 — Администратор ИРУЦ
1.2.643.3.131.1000.0.2 — Оператор ИРУЦ
1.2.643.3.131.1059.0.3 — ЮЛ и ИП
1.2.643.3.131.1000.0.6 — Веб-сервер ИРУЦ
1.2.643.3.131.1000.0.7 — Доверенный УЦ
1.2.643.3.131.1000.0.8 — Сервер регистрации ИРУЦ
1.2.643.3.131.1000.0.9 — УЦ организатора системы.
1.2.643.3.131.1000.0.11 — Специализированный оператор связи
1.2.643.3.131.1000.0.13 — ЦСДИ

Квалификация подписи

1.2.643.3.131.1059.0.3.1 — руководитель
1.2.643.3.131.1059.0.3.2 — главный бухгалтер
1.2.643.3.131.1059.0.3.3 — руководитель и главный бухгалтер
1.2.643.3.131.1059.0.3.4 — уполномоченный представитель
1.2.643.3.131.1059.0.3.5 — индивидуальный предприниматель
1.2.643.3.131.1059.0.3.6 — ответственный исполнитель

Пользователь сервисов системы

1.2.643.3.131.1059.0.3.1.0 - сервисы не используются
1.2.643.3.131.1059.0.3.2.0 - сервисы не используются
1.2.643.3.131.1059.0.3.3.0 - сервисы не используются
1.2.643.3.131.1059.0.3.4.0 - сервисы не используются
1.2.643.3.131.1059.0.3.5.0 - сервисы не используются
1.2.643.3.131.1059.0.3.6.0 - сервисы не используются
1.2.643.3.131.1059.0.3.1.1 - используется сервис ИОН on-line
1.2.643.3.131.1059.0.3.2.1 - используется сервис ИОН on-line
1.2.643.3.131.1059.0.3.3.1 - используется сервис ИОН on-line
1.2.643.3.131.1059.0.3.4.1 - используется сервис ИОН on-line

1.2.643.3.131.1059.0.3.5.1 - используется сервис ИОН on-line
1.2.643.3.131.1059.0.3.6.1 - используется сервис ИОН on-line

8.1.7. 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 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".

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 34.11/34.10-2001
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 сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
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: i. Тип участника (один вариант из списка) 1. Юридическое лицо(OID 1.2.643.6.3.1.2.1) 2. Физическое лицо(OID 1.2.643.6.3.1.2.2) 3. Индивидуальный предприниматель(OID 1.2.643.6.3.1.2.3) ii. Тип организации: 1. Участник размещения заказа(OID 1.2.643.6.3.1.3.1) iii. Полномочия (множественный выбор): 1. Администратор организации(OID 1.2.643.6.3.1.4.1) 2. Уполномоченный специалист(OID 1.2.643.6.3.1.4.2) 3. Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3)
Application Policy	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 сертификата	Идентификатор закрытого ключа владельца 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).

4.2.4. 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).

4.2.5. 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)

Тип участника (один вариант из списка)

1. Юридическое лицо (OID 1.2.643.6.3.1.2.1)
2. Физическое лицо (OID 1.2.643.6.3.1.2.2)
3. Индивидуальный предприниматель (OID 1.2.643.6.3.1.2.3)

Тип организации:

1. Участник размещения заказа (OID 1.2.643.6.3.1.3.1)

Полномочия (множественный выбор):

1. Администратор организации (OID 1.2.643.6.3.1.4.1)
2. Уполномоченный специалист (OID 1.2.643.6.3.1.4.2)
3. Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3)

4.3. Требования к составу списка отозванных сертификатов, публикуемого удостоверяющим центром

4.3.1. 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 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
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
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.

10.2.5. 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. 2.2).

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

Директору ООО“Мостинфо”
Вилисовой И.Б.
620075, город Екатеринбург,
ул. Первомайская, дом 15. оф.1204

«____» _____ 20____ г.

Заявление
на изготовление квалифицированного сертификата ключа подписи
(для юридических лиц и ИП)

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

Просим создать ключ электронной подписи и ключ проверки электронной подписи изготовить квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

Organization (O)	Сокращенное наименование организации в соответствии с выпиской	
Title (T)	Должность	
CommonName (CN)	Фамилия, Имя, Отчество	
OrganizationUnit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Область	
Street	Название улицы, номер дома	
Contry (C)	RU	
E-Mail (E)	Адрес электронной почты	
SNILS	Страховой номер индивидуального лицевого счёта уполномоченного представителя	
OGRN	Основной государственный регистрационный номер юридического лица	
INN	Индивидуальный номер налогоплательщика юридического лица, перед которым находятся две цифры ноль	

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 соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» в целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО «Мостинфо» (формирования общедоступных справочников сертификатов ключей подписей, списков отозванных сертификатов ключей подписей) своей волей и в своем интересе выражаю согласие ООО «Мостинфо», на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) с использованием средств автоматизации или без использования таких средств моих персональных данных: фамилия, имя, отчество, адрес места жительства по паспорту, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), место работы, должность, служебный телефон и иные сведения, необходимые для исполнения целей настоящего регламента.

Согласие вступает в силу с момента его подписания, действует в течение 1года и может быть отозвано мною в любое время на основании моего письменного заявления.

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

Приложение №2 к Регламенту

Заявление на изготовление квалифицированного сертификата ключа подписи для физических лиц

Директору ООО“Мостинфо”
Вилисовой И.Б.
620075, город Екатеринбург,
ул. Первомайская, дом 15. оф.1204

«____» _____ 20____ г.

Заявление
на изготовление квалифицированного сертификата ключа подписи
(для физических лиц)

Я, _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта
_____
(кем и когда выдан)

Прошу создать ключ электронной подписи и ключ проверки электронной подписи изготовить квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

CommonName (CN)	Фамилия, Имя, Отчество	
Locality (L)	Город	
State (S)	Область	
Contry (C)	RU	
E-Mail (E)	Адрес электронной почты	
SNILS	Страховой номер индивидуального лицевого счёта	
INN	Индивидуальный номер налогоплательщика юридического лица, перед которым находятся две цифры ноль	

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 соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» в целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО «Мостинфо» (формирования общедоступных справочников сертификатов ключей подписей, списков отозванных сертификатов ключей подписей) своей волей и в своем интересе выражаю согласие ООО «Мостинфо», на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) с использованием средств автоматизации или без использования таких средств моих персональных данных: фамилия, имя, отчество, адрес места жительства по паспорту, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), место работы, должность, служебный телефон и иные сведения, необходимые для исполнения целей настоящего регламента.

Согласие вступает в силу с момента его подписания, действует в течение 1года и может быть отозвано мною в любое время на основании моего письменного заявления.

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

Приложение №3 к Регламенту

Форма доверенности на получение ЭП

Директору ООО “Мостинфо”
Вилисовой И.Б.
620075, город Екатеринбург
ул. Первомайская дом 15, оф. 1204

Доверенность

Город _____ «_____» _____ 20___ г.

_____
Полное наименование организации, включая организационно-правовую форму

В лице _____
должность руководителя юридического лица

_____
ФИО

действующего на основании _____ уполномочивает
основание полномочий

_____
ФИО

паспорт серии_____ №_____ выдан _____ «__» _____20__ год

1. Предоставить в Удостоверяющий центр ООО «Мостинфо» необходимые документы, определенные Регламентом Удостоверяющего центра ООО «Мостинфо» для регистрации в Удостоверяющем центре ООО «Мостинфо».

2. Получить ключевую информацию, сертификат ключа подписи Пользователя Удостоверяющего центра на _____, а также
(фамилия, имя, отчество владельца СКП)

иные документы, определенные Регламентом Удостоверяющего центра ООО "Мостинфо".

3. Получить средства криптографической защиты информации (СКЗИ) в ООО ”Мостинфо” и выполнить все необходимые действия, связанные с исполнением настоящего поручения, в том числе с правом подписи в журнале поэкземплярного учета СКЗИ и прочих учетных документах

4. Представитель наделяется правом расписываться на копии сертификата ключа подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

5. Заключить договор и подписать финансовые документы (в рамках выполненных работ и оказанных услуг по договору).

Настоящая доверенность действительна по « » _____ 20___ года и выдана без права передоверия.

Подпись лица получившего доверенность _____
(подпись)

Руководитель _____
(подпись) М.П.

Приложение №4 к Регламенту

Форма заявления на прекращение действия Сертификата

Директору ООО “Мостинфо”
Вилисовой И.Б.
620075, город Екатеринбург
ул. Первомайская дом 15, оф. 1204

ЗАЯВЛЕНИЕ НА ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

Город _____ «_____» _____ 20__ г.

Прошу прекратить действие квалифицированного сертификата ключа проверки электронной подписи, серийный номер:

_____, выданный

_____

(ФИО владельца сертификата физического лица или наименование юридического лица, ОГРН, ФИО уполномоченного представителя, который указан в сертификате)

в связи с _____.

(указать причину: нарушение конфиденциальности ключа подписи, прекращение работы и т.д.).

для юридических лиц:
Владелец Сертификата
(наименование, ОГРН) _____ _____
___

(наименование, ОГРН) (подпись уполномоченного лица и печать, документ-основание полномочий уполномоченного лица) (расшифровка подписи)

для физических лиц:

Владелец Сертификата _____ _____
(Ф.И.О) (расшифровка подписи)

Настоящим подтверждаю, что Заявление на прекращение действия квалифицированного сертификата ключа проверки электронной подписи получено, личность

_____

(указать ФИО обратившегося лица полностью)

идентифицирована, сведения, указанные в Заявлении, проверены.

Доверенное лицо Удостоверяющего центра _____ _____
(подпись) (расшифровка подписи)