Утвержден
Приказом ООО «Гвард-Информ»
№ 1/05 от 23.05.2016 г.

РЕГЛАМЕНТ
Удостоверяющего центра
ООО «Гвард-Информ»
по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)

Редакция №2

г. Тула
2016

1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «Гвард-Информ», именуемое в дельнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Тула. Свидетельство о регистрации № ГТ 003657, выдано 01.03.2002г. Тульской городской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1027100971182 от 01.03.2002г.

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании **свидетельства об аккредитации удостоверяющего центра №99**, выданного Минкомсвязи России (федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи) и **лицензии выданной УФСБ России по Тульской области ЛСЗ №0004004 Рег.№974Н** на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Реквизиты ООО «Гвард-Информ»:
Полное наименование: Общество с ограниченной ответственностью «Гвард-Информ»
Юридический адрес: 300046 г. г.Тула, пр. Ленина д.46 оф.322.
Фактический адрес: 300046 г. г.Тула, пр. Ленина д.46 оф.407.
Адрес для корреспонденции: 300046 г. г.Тула, пр. Ленина д.46 оф.407.
Банковские реквизиты р/с 40702810802000018701
в Ярославском филиале ПАО ”Промсвязьбанк” г. Ярославль БИК 047888760
к/с 30101810300000000760
ИНН/КПП: 7107065081/710701001
ОГРН: 1027100971182

Контактные телефоны, факс, адрес электронной почты:

- тел./факс (4872) 361-300; e-mail: qca@ginf.ru, info@ginf.ru

2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральным законом «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями:

- по обеспечению создания ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, аннулирование, прекращение, приостановление и возобновление действия) сертификатами ключей проверки электронной подписи Операторов Удостоверяющего центра;
- на аннулирование, прекращение, приостановление и возобновление действия сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра;
- на заверение копии сертификатов ключей проверки электронной подписи Операторов Удостоверяющего центра на бумажном носителе.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в соответствии с законодательством Российской Федерации Удостоверяющим центом выдан сертификат ключа проверки электронной подписи.

Возобновление действия сертификата ключа проверки электронной подписи (возобновление действия сертификата) – отмена приостановления действия сертификата проверки электронной подписи и признание его действительным. Порядок возобновления действия сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

Запрос на сертификат ключа проверки электронной подписи (Запрос на сертификат) – электронный файл содержащий данные запрашиваемые для изготовления сертификата ключа проверки электронной подписи, в том числе запрашиваемые ограничения использования сертификата ключа проверки электронной подписи и следующие данные, относящиеся к лицу, желающему стать владельцем сертификата ключа проверки электронной подписи:

- ключ проверки электронной подписи, связанный с ключом электронной подписи, которым владеет данное лицо;
- идентификационные данные лица, подлежащие внесению в сертификат ключа проверки электронной подписи.

Клиент Уполномоченной организации - Пользователь Удостоверяющего центра, являющийся Владельцем сертификата ключа проверки электронной подписи, решение по созданию которого было принято Оператором Удостоверяющего центра.

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

Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи) если:

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;

- сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует на указанный момент времени.

Ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, использующийся Удостоверяющим центром для создания сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

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

Копия сертификата ключа проверки электронной подписи - документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра, либо подписанный Оператором Удостоверяющего центра и заверенный печатью Уполномоченной организации. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

Оператор Удостоверяющего центра – физическое лицо, являющееся сотрудником Уполномоченной организации, действующее от имени Уполномоченной организации по обеспечению создания, выдачи и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра.

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец ключа проверки электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 10:00 по 18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

Сертификат ключа проверки электронной подписи - электронный документ, выданный Удостоверяющим центром или доверенным лицом Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;
- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие и действие его не приостановлено.

Сертификат ключа проверки электронной подписи Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи Удостоверяющего центра в созданных им сертификатах ключей проверки электронной подписи и списках отозванных сертификатов.

Список отозванных сертификатов (СОС) – электронный документ с квалифицированной электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы, действие которых прекращено и действие которых приостановлено.

Удостоверяющий центр – ООО «Гвард-Информ», осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи». Удостоверяющий центр с момента аккредитации уполномоченным федеральным органом исполнительной власти Российской Федерации в сфере использования электронной подписи осуществляет создание и выдачу квалифицированных сертификатов ключей проверки электронной подписи.

Уполномоченная организация – юридическое лицо, заключившее с Удостоверяющим центром договор, наделяющий данное юридическое лицо полномочиями по обеспечению создания, выдачи и управлению сертификатами ключей проверки электронных подписей Пользователей Удостоверяющего центра.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Cryptographic Message Syntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляют свою работу в соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа проверки электронной подписи.

3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи (Схема обслуживания: с уполномоченной организацией), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

3.1.2. Сторонами Регламента (далее Стороны) являются Удостоверяющий центр - ООО «Гвард-Информ» и Уполномоченная организация.

3.1.3. Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

3.2. Применение Регламента

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

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

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

3.3. Изменение Регламента

3.3.1. Внесение изменений в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

3.3.2. Уведомление о внесении изменений в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений на сайте Удостоверяющего центра по адресу: http://qca.ginf.ru/reglament/reglamentAO.pdf

3.3.3. Все изменения, вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении одного месяца с даты размещения указанных изменений в Регламенте на сайте Удостоверяющего центра по адресу - http://qca.ginf.ru/reglament/reglamentAO.pdf.

3.3.4. Все изменения, вносимые Удостоверяющим центром в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативно-правовых актов, повлекших изменение законодательства Российской Федерации.

3.3.5. Любые изменения в Регламенте с момента вступления в силу равно распространяются на все Уполномоченные организации, в том числе заключившие с Удостоверяющим центром договор до даты вступления изменений в силу изменений в Регламент.

3.3.6. Все приложения к настоящему Регламенту являются его составной и неотъемлемой частью.

4. Предоставление информации

4.1. Удостоверяющий центр осуществляет свою деятельность в качестве аккредитованного удостоверяющего центра на основании решения Минкомсвязи России, являющегося федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. С информацией по аккредитации Удостоверяющего центра можно ознакомиться на официальном сайте Минкомсвязи России.

4.2. Удостоверяющий центр осуществляет свою деятельность в соответствии с лицензией, выданной УФСБ России по Тульской области ЛСЗ №0004004 Рег.№974Н, копия которой может быть предоставлена Уполномоченной организации по запросу.

4.3. Уполномоченная организация обязана предоставить Удостоверяющему центру следующие документы:

При подаче заявления за выдачу сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра:

- выписку из Единого государственного реестра юридических лиц, сформированную не ранее, чем за три месяца до момента предоставления в Удостоверяющий центр. Выписка может быть предоставлена на бумажном носителе, прошитая и заверенная печатью ФНС России, либо в электронной форме, подписанная электронной подписью ФНС России;
- нотариально заверенную копию Свидетельства о внесении записи в ЕГРЮЛ, либо незаверенную копию с предъявлением оригинала;
- нотариально заверенную копию Свидетельства о постановке на учет в налоговом органе, либо незаверенную копию с предъявлением оригинала;
- нотариально заверенную копию документа, признаваемого в соответствии с законодательством Российской Федерации документом, удостоверяющим личность либо незаверенную копию с предъявлением оригинала - для Оператора Удостоверяющего центра;
- нотариально заверенную копию страхового свидетельства обязательного (государственного) пенсионного страхования - личность либо незаверенную копию с предъявлением оригинала - для Оператора Удостоверяющего центра;
- документы, подтверждающие финансовое обеспечение своей ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи и идентифицирующей владельца сертификата ключа проверки электронной подписи;
- иные документы, установленные Регламентом Удостоверяющего центра, а также дополнительные документы по усмотрению Удостоверяющего центра;

В отношении сертификата ключа проверки электронной подписи, создаваемого Клиенту Уполномоченной организации – юридическому лицу:

- выписку из Единого государственного реестра юридических лиц, сформированную не ранее, чем за три месяца до момента подачи заявления на сертификат, в электронной форме, подписанную электронной подписью ФНС России;
- копию Свидетельства о внесении записи в ЕГРЮЛ, заверенную

Оператором Удостоверяющего центра;

- копию Свидетельства о постановке на учет в налоговом органе, заверенную Оператором Удостоверяющего центра;
- копию документа, признаваемого в соответствии с законодательством Российской Федерации документом, удостоверяющим личность, заверенную Оператором Удостоверяющего центра - для того физического лица, которое указывается в сертификатах ключей проверки электронной подписи наряду с указанием наименования юридического лица;
- копию страхового свидетельства обязательного (государственного) пенсионного страхования, заверенную Оператором Удостоверяющего центра - для того физического лица, которое указывается в сертификатах ключей проверки электронной подписи наряду с указанием наименования юридического лица;
- копию документа, подтверждающего правомочия физического лица обращаться за получением сертификата ключа проверки электронной подписи данного юридического лица.
- иные документы, установленные Регламентом Удостоверяющего центра, а также дополнительные документы по усмотрению Удостоверяющего центра;

В отношении сертификата ключа проверки электронной подписи, создаваемого Клиенту Уполномоченной организации – физическому лицу:

- копию документа, признаваемого в соответствии с законодательством Российской Федерации документом, удостоверяющим личность, заверенную Оператором Удостоверяющего центра;
- копию страхового свидетельства обязательного (государственного) пенсионного страхования, заверенную Оператором Удостоверяющего центра;

5. Права и обязанности сторон

5.1. Удостоверяющий центр обязан:

5.1.1. Предоставить Оператору Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

5.1.2. Использовать для создания ключа электронной подписи Удостоверяющего центра и формирования электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

5.1.3. Использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

5.1.4. Принять меры по защите ключа электронной подписи Удостоверяющего центра от несанкционированного доступа.

5.1.5. Организовать свою работу по московскому времени.

5.1.6. Обеспечить уникальность идентификационных данных Операторов и Пользователей Удостоверяющего центра, заносимых в сертификаты ключей проверки электронной подписи.

5.1.7. Создать сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра по заявлению на создание сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.8. Обеспечить уникальность серийных номеров создаваемых сертификатов ключей проверки электронной подписи.

5.1.9. Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Операторов и Пользователей Удостоверяющего центра.

5.1.10. Обеспечить сохранение в тайне созданного ключа электронной подписи Оператора Удостоверяющего центра.

5.1.11. Прекратить, приостановить и возобновить действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по соответствующему заявлению на прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.12. Обеспечить прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в соответствии с порядком, определенным в настоящем Регламенте.

5.1.13. Прекратить действие сертификатов ключей проверки электронной подписи Операторов и Пользователей Удостоверяющего центра, если истек установленный срок, на который действие данных сертификатов было приостановлено.

5.1.14. Прекратить действие сертификатов ключей проверки электронной подписи Операторов и Пользователей Удостоверяющего центра в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с

использованием которого были созданы сертификаты ключей проверки электронной подписи Операторов и Пользователей Удостоверяющего центра.

5.1.15. Официально уведомить об аннулировании, прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации списка отозванных сертификатов.

5.1.16. Обеспечить публикацию актуального списка отозванных сертификатов по адресам: http://qca.ginf.ru/cdp/ и http://ginf-qca.ru/cdp/. Период публикации списка отозванных сертификатов – 7 календарный дней.

5.1.17. Предоставить Уполномоченной организации необходимые права для осуществления регистрации пользователей в Удостоверяющем центре, формирования и отправки в Удостоверяющий центр заявок в электронной форме на создание и управление сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.2. Уполномоченная организация обязана:

5.2.1. С целью обеспечения гарантированного ознакомления Уполномоченной организации с полным текстом изменений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу http://q.cryptopro.ru/reglament/reglamentAO.pdf за сведениями об изменениях в Регламенте.

5.2.2. Известить Удостоверяющий центр об изменениях реквизитов Уполномоченной организации и по требованию Удостоверяющего Центра предоставить документы, указанные в п.4.3 настоящего Регламента, в течение 5-ти рабочих дней с момента регистрации изменений.

5.2.3. Обеспечить работоспособность и неизменность программной среды на рабочем месте Оператора, подготовленного с участием Удостоверяющего центра.

5.2.4. Обеспечивать соблюдение требований безопасности на используемые средства криптографической защиты информации и действующего законодательства Российской Федерации в области защиты информации и рабочем месте Оператора.

5.2.5. Заверять печатью Уполномоченной организации копии его сертификатов ключей проверки электронной подписи Клиентов Уполномоченной организации.

5.2.6. Оператор Удостоверяющего центра, являющийся полномочным представителем Уполномоченной организации, обязан:

5.2.6.1. При взаимодействии со средствами обеспечения деятельности Удостоверяющего центра использовать только те средства, которые были предоставлены Удостоверяющим центром.

5.2.6.2. Обеспечить конфиденциальность ключей электронных подписей.

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

5.2.6.4. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
5.2.6.5. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.
5.2.6.6. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
5.2.6.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
5.2.6.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.
5.2.6.9. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.
5.2.6.10. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
5.2.6.11. Уничтожить личный ключ электронной подписи в соответствии с эксплуатационной документацией на СКЗИ сразу по окончании срока его действия.
5.2.6.12. Устанавливать личность заявителей – физических лиц, желающих стать Клиентом Уполномоченной организации и обратившихся в Уполномоченную организацию за обеспечением создания и выдачи сертификата ключа проверки электронной подписи;
5.2.6.13. Получить от лиц, выступающих от имени заявителей - юридических лиц, желающих стать Клиентом Уполномоченной организации и обратившихся в Уполномоченную организацию за обеспечением создания и выдачи сертификата ключа проверки электронной подписи, подтверждение правомочия обращаться за получением сертификата ключа проверки электронной подписи.

5.2.6.14. При обращении лиц, желающих стать Клиентом Уполномоченной организации, получать от них оригиналы (либо нотариально заверенные копии) документов, подтверждающих достоверность информации, предоставленной заявителем для включения в сертификат ключа проверки электронной подписи, изготавливать и заверять их копии для предоставления в Удостоверяющий центр согласно списку, указанному в пункте 4.3.

5.2.6.15. Информировать лиц, желающих стать Клиентом Уполномоченной организации, о необходимости обработки их персональных данных Удостоверяющим центром и получать их письменное согласие на обработку персональных данных по форме, с согласованной с Удостоверяющим центром.

5.2.6.16. Знакомить лиц, желающих стать Клиентом Уполномоченной организации, с положениями настоящего Регламента, касающихся Пользователей Удостоверяющего центра.

5.2.6.17. Включать в договора с лицами, желающими стать Клиентом Уполномоченной организации, обязанности Пользователя Удостоверяющего центра, указанные в Приложении №11.

5.2.6.18. Одновременно с выдачей сертификата ключа проверки электронной подписи Клиенту Уполномоченной организации выполнить следующие процедуры:

- распечатать в двух экземплярах на бумажных носителях информацию, содержащуюся в сертификате ключа проверки электронной подписи, представленную в виде копии сертификата, оформленной по форме Приложения №8, заверить их личной подписью и печатью Уполномоченной организации;
- под расписку ознакомить Клиента Уполномоченной организации с информацией, содержащейся в сертификате ключа проверки электронной подписи, представленную в виде копии сертификата, оформленной по форме Приложения №8;
- одну копию сертификата, оформленную по форме Приложения №8 и заверенную подписями, передать Клиенту Уполномоченной организации, а вторую сохранить у себя, направив копию в Удостоверяющий центр;
- выдать Клиенту Уполномоченной организации руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи по форме Приложения №12

5.3. Удостоверяющий центр имеет право:

5.3.1. Отказать в создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае ненадлежащего оформления заявления на создание сертификата ключа проверки электронной подписи.

5.3.2. Отказать в создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае не предоставления и/или

ненадлежащего предоставления документов, установленных п. 4.3 настоящего Регламента.

5.3.3. Отказать в прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи.

5.3.4. Отказать в прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату.

5.3.5. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с обязательным уведомлением Оператора Удостоверяющего центра и указанием обоснованных причин.

5.3.6. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Клиента Уполномоченной организации в случае непредставления Уполномоченной организацией документов согласно п. 4.3 в течении 30 дней с момента создания сертификата ключа проверки электронной подписи.

5.3.7. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Клиента Уполномоченной организации с обязательным уведомлением Оператора Удостоверяющего центра об этом и указанием обоснованных причин.

5.3.8. Отказать в создании и управлении сертификатами ключей проверки электронной подписи по заявкам Оператора Удостоверяющего центра до получения документов, установленных п. 4.3 настоящего Регламента.

5.3.9. Отказать в создании сертификата ключа проверки электронной подписи по заявкам Оператора Удостоверяющего центра в случае, если запрашиваемые для внесения в сертификат ключа проверки электронной подписи данные не соответствуют ограничениям, указанным в Приложении №10.

5.3.10. В одностороннем порядке прекратить действие сертификата ключа проверки электронной подписи Клиента Уполномоченной организации в случае Прямого обращения Пользователя Удостоверяющего центра в Удостоверяющий центр, с обязательным уведомлением Оператора Удостоверяющего центра об этом.

5.4. Уполномоченная организация имеет право:

5.4.1. Заверять печатью Уполномоченной организации копии сертификатов ключей проверки электронной подписи, решение по созданию которых было принято

Оператором Удостоверяющего центра, являющимся полномочным лицом Уполномоченной организации.

5.4.2. Оператор Удостоверяющего центра имеет право:

5.4.2.1. Получить копию сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра на бумажном носителе, заверенную Удостоверяющим центром.

5.4.2.2. Заверять собственноручной подписью копии сертификатов ключей проверки электронной подписи, решение по созданию которых было принято Оператором Удостоверяющего центра.

5.4.2.3. Принимать решения по созданию и выдаче сертификатов ключей проверки электронной подписи.

5.4.2.4. Прекращать, приостанавливать и возобновлять действие сертификатов ключей проверки электронной подписи, решение по созданию которых было принято Оператором Удостоверяющего центра.

5.4.3. Оператор Удостоверяющего центра и Клиент Уполномоченной организации имеют право:

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

5.4.3.2. Применять список отозванных сертификатов ключей проверки электронных подписей, созданный Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

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

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

6. Ответственность сторон

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

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

6.3. Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях и документах, исходящих от Уполномоченной организации.

6.4. Удостоверяющий центр несет ответственность за убытки при использовании созданного Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи в том случае, если данные убытки возникли по причине нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра.

6.5. Вся ответственность по занесению данных в сертификаты ключей проверки электронной подписи, принятию решений по созданию, выдаче и управлению сертификатами ключей проверки электронной подписи, формированию копий сертификатов ключей проверки электронной подписи полностью возлагается на Уполномоченную организацию.

6.6. Возмещение убытков не освобождает Стороны от выполнения обязательств в натуре.

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

7. Разрешение споров

7.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Уполномоченная организация.

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

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

7.4. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде Тульской области.

8. Порядок предоставления и пользования услугами Удостоверяющего центра

8.1. Общий порядок пользования услугами Удостоверяющего центра

Уполномоченная организация в лице Оператора Удостоверяющего центра осуществляет формирование ключей электронной подписи, принятие решений по созданию, выдаче и управлению сертификатами ключей проверки электронной подписи с использованием специализированных программных средств, предоставляемых Удостоверяющим центром Уполномоченной организации, и применения квалифицированной электронной подписи Оператора Удостоверяющего центра.

Удостоверяющий центр осуществляет действия по созданию и управлению сертификатами ключей проверки электронной подписи, решение по которым принимает Оператор Удостоверяющего центра, на основании электронных заявлений, подписанных квалифицированной электронной подписью Оператора Удостоверяющего центра. При этом электронное заявление, подписанное квалифицированной электронной подписью, признается действительным и принимается Удостоверяющим центром при одновременном выполнении следующих условий:

- Выполнены условия признания квалифицированной электронной подписи в заявлении Оператора Удостоверяющего центра;
- Квалифицированная электронная подпись в заявлении сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Оператора Удостоверяющего центра, а именно: сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.2.643.2.2.34.5 – «Оператор Центра регистрации».

Для взаимодействия с Удостоверяющим центром Уполномоченная организация в лице Оператора Удостоверяющего центра должна стать владельцем сертификата ключа проверки электронной подписи.

Формирование ключей электронной подписи, создание, выдача и управление сертификатами Операторов Удостоверяющего центра осуществляется в соответствии с данным разделом настоящего Регламента.

8.2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центр осуществляется либо с формированием ключей электронной подписи Администратором удостоверяющего центра, либо по Запросу на сертификат, после самостоятельного формирование ключей электронной подписи Оператором Удостоверяющего центра.

8.2.1. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с формированием ключей электронной подписи Администратором Удостоверяющего центра

Создание сертификата ключа проверки электронной подписи с формированием ключей электронной подписи Администратором Удостоверяющего центра

осуществляется на основании заявления на создание сертификата ключа проверки электронной подписи с формированием ключей электронной подписи Администратором удостоверяющего центра по форме Приложения №1-А и доверенности Оператора Удостоверяющего центра по форме Приложения №2.

Предоставление заявительных документов для создания сертификата ключа проверки электронной подписи, а также получение сформированных Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, может быть осуществлено:

- Оператором Удостоверяющего центра;
- Представителем Уполномоченной организации на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, оформленной по форме Приложения №3-А к настоящему Регламенту;

Администратор Удостоверяющего центра на основе предоставленных заявительных документов выполняет действия по формированию ключа электронной подписи и созданию сертификата ключа проверки электронной подписи. Ключ электронной подписи и сертификат ключа проверки электронной подписи записываются на предоставляемый заявителем ключевой носитель.

Администратор Удостоверяющего центра передает сформированный ключевой носитель заявителю и распечатывает на бумажном носителе информацию, содержащуюся в созданном сертификате ключа проверки электронной подписи, представленную в виде копии сертификата, оформленной по форме Приложения № 8. Заявитель под расписку ознакамливается с информацией из сертификата ключа проверки электронной подписи.

Одновременно с выдачей сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра передает Оператору Удостоверяющего центра руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Создание и выдача сертификатов ключей проверки электронной подписи Оператору Удостоверяющего центра осуществляется Удостоверяющим центром в день прибытия заявителя. День прибытия заявителя согласовывается с Администратором Удостоверяющего центра. Удостоверяющий центр вправе отказать в создании сертификатов по заявлениям, поступившим в Удостоверяющим центр без согласования дня прибытия заявителя.

8.2.2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по Запросу на сертификат

С целью создания сертификата ключа проверки электронной подписи по Запросу на сертификат Оператор Удостоверяющего центра самостоятельно формирует ключ электронной подписи и связанный с ним ключ проверки электронной подписи, который включает в Запрос на сертификат, формируемый в формате стандарта PKCS#10.

Создание сертификата ключа проверки электронной подписи по Запросу на сертификат осуществляется на основании заявления на создание сертификата ключа

проверки электронной подписи по Запросу на сертификат по форме Приложения №1-Б и доверенности Оператора Удостоверяющего центра по форме Приложения №2, с приложением непосредственно Запроса на сертификат на носителе Оператора Удостоверяющего центра.

Предоставление заявительных документов для создания сертификата ключа проверки электронной подписи, а также получение сформированных Удостоверяющим центром сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, может быть осуществлено:

- Оператором Удостоверяющего центра;
- Представителем Уполномоченной организации на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, оформленной по форме Приложения №3-Б к настоящему Регламенту;

Администратор Удостоверяющего центра осуществляет сравнение содержимого файла Запроса на сертификат с предоставленным заявительным комплектом документов и принимает решение о создании сертификата ключа проверки электронной подписи Оператору Удостоверяющего центра.

В случае отказа в создании сертификата ключа проверки электронной подписи Оператор Удостоверяющего центра уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Администратор Удостоверяющего центра выполняет действия по созданию сертификата ключа проверки электронной подписи и передает созданный сертификат ключа проверки электронной подписи на предоставленный Оператором Удостоверяющего центра носитель, после чего распечатывает на бумажном носителе информацию, содержащуюся в созданном сертификате ключа проверки электронной подписи, представленную в виде копии сертификата, оформленной по форме Приложения № 8. Заявитель под расписку ознакамливается с информацией из сертификата ключа проверки электронной подписи.

Одновременно с выдачей сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра передает Оператору Удостоверяющего центра руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Создание и выдача сертификатов ключей проверки электронной подписи Оператору Удостоверяющего центра осуществляется Удостоверяющим центром в день прибытия заявителя. День прибытия заявителя согласовывается с Администратором Удостоверяющего центра. Удостоверяющий центр вправе отказать в создании сертификатов по заявлениям, поступившим в Удостоверяющим центр без согласования дня прибытия заявителя.

8.3. Прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Удостоверяющий центр прекращает действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в следующих случаях:

- при прекращении действия настоящего Регламента в отношении Уполномоченной организации по усмотрению Удостоверяющего центра;
- по истечении срока, на который действие сертификата было приостановлено;
- по заявлению владельца сертификата ключа проверки электронной подписи;
- в связи с аннулированием сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу.
- по истечении срока действия сертификата ключа проверки электронной подписи;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи;

В случае прекращения действия настоящего Регламента, истечения срока, на который действие сертификата было приостановлено, по заявлению владельца сертификата, по решению суда, вступившего в законную силу Удостоверяющий центр, официально уведомляет владельца сертификата и всех Пользователей Удостоверяющего центра о прекращении действия сертификата ключа проверки электронной подписи не позднее одного рабочего дня с момента наступления описанного события.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point сертификата ключа проверки электронной подписи.

В случае прекращения действия сертификата ключа проверки электронной подписи по истечению срока его действия временем прекращения действия сертификата ключа проверки электронной подписи признается время, хранящееся в поле notAfter поля Validity сертификата ключа проверки электронной подписи. В этом случае информация о сертификате, действие которого прекращено, в список отозванных сертификатов не заносится.

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра временем прекращения действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра признается время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, фиксирующееся Удостоверяющим центром. При этом информация о сертификате ключа проверки электронной подписи Оператора Удостоверяющего центра в список отозванных сертификатов не заносится.

8.3.1. Прекращение действия сертификата ключа проверки электронной подписи по заявлению Оператора Удостоверяющего центра

Заявление на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра предоставляется в Удостоверяющий центр по форме Приложения №4 настоящего регламента.

После получения Удостоверяющим центром заявления на прекращение действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на прекращение действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в прекращении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Администратор Удостоверяющего центра осуществляет прекращение действия сертификата ключа проверки электронной подписи.

8.4. Приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Удостоверяющий центр приостанавливает действие сертификата ключа проверки электронной подписи в следующих случаях:

- по заявлению владельца сертификата ключа проверки электронной подписи;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

Действие сертификата ключа проверки электронной подписи приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа проверки электронной подписи составляет 15 (Пятнадцать) дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то данный сертификат прекращает своё действие.

Официальным уведомлением о факте приостановления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, и изданного не ранее времени наступления произошедшего случая. Временем приостановления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point сертификата ключа проверки электронной подписи.

8.4.1. Приостановление действия сертификата ключа проверки электронной подписи по заявлению Оператора Удостоверяющего центра

Подача заявления в Удостоверяющий центр на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра предоставляется в Удостоверяющий центр по форме Приложения №5 настоящего Регламента.

После получения Удостоверяющим центром заявления на приостановление действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в приостановление действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Администратор Удостоверяющего центра осуществляет приостановление действия сертификата ключа проверки электронной подписи.

8.4.2. Приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по решению Удостоверяющего центра

Удостоверяющий центр вправе приостановить действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в следующих случаях:

- нарушения конфиденциальности или подозрения в нарушении конфиденциальности соответствующего ключа электронной подписи;
- неисполнения Оператором Удостоверяющего центра обязательств по настоящему Регламенту;
- в случаях, предусмотренных договором между Удостоверяющим центром и Уполномоченной организацией

После приостановления действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра сообщает Оператору Удостоверяющего центра о наступлении события, повлекшего приостановление действия сертификата, и уведомляет его о том, что действие сертификата приостановлено.

8.5. Возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра только по заявлению его владельца и только в том случае, если действие сертификата ключа проверки электронной подписи было приостановлено.

Заявление на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра предоставляется в Удостоверяющий центр по форме Приложения № 6 настоящего Регламента.

После получения Удостоверяющим центром заявления на возобновление действия сертификата ключа проверки электронной подписи Администратор

Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на возобновление действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в возобновлении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Администратор Удостоверяющего центра осуществляет возобновление действия сертификата ключа проверки электронной подписи.

Официальным уведомлением о факте возобновления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point.

8.6. Проверка подлинности электронной подписи в электронном документе

По желанию Уполномоченной организации Удостоверяющий центр осуществляет проведение экспертных работ по проверке подлинности электронной подписи в электронном документе.

В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то Удостоверяющий центр обеспечивает проверку подлинности электронной подписи в электронном документе. Решение о соответствии формата представления электронной подписи (формата представления электронного документа с электронной подписью) стандарту CMS принимает Удостоверяющий центр.

Для проверки подлинности электронной подписи в электронных документах Уполномоченная организация подает заявление в Удостоверяющий центр по форме, приведенной в Приложении № 7 настоящего Регламента. Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные владельца сертификата, электронную подпись которого необходимо проверить в электронном документе;
- дата и время формирования электронной подписи электронного документа;
- дата и время, на момент наступления которых требуется проверить подлинность электронной подписи (в том случае, если информация о дате и времени подписания электронного документа отсутствует).

Обязательным приложением к заявлению на проверку подлинности электронной подписи в электронном документе является носитель, содержащий:

- сертификат ключа проверки электронной подписи, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе – в виде файла стандарта CMS;
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

Проведение работ по проверке подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом проведения работ по проверке подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- данные, предоставленные комиссии для проведения проверки.
- результат проверки электронной подписи электронного документа.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по проверке подлинности электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет 20 (Двадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по проверке подлинности электронной подписи осуществляется в рамках заключения отдельного договора между Удостоверяющим центром и Уполномоченной организацией. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором.

9. Форма сертификата ключа проверки электронной подписи, списка отозванных сертификатов и сроки действия ключевых документов

9.1. Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром

Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи», с учетом технических ограничений на длину полей, указанных в Приложении 10.

Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи заносится следующая информация:

- расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) - набор объектных идентификаторов (OID), устанавливающих ограничения на применение квалифицированной электронной подписи совместно с сертификатом ключа проверки электронной подписи (если такие ограничения установлены);
- расширение CRL Distribution Point (Точка распространения списка отозванных сертификатов) - набор адресов точек распространения списков отозванных сертификатов;
- расширение Authority Information Access (Доступ к информации о центре) - Адрес размещения сертификата Удостоверяющего центра;
- иные расширения по усмотрению Удостоверяющего центра.

По согласованию сторон, в выдаваемые сертификаты так же может заноситься иная информация о владельце квалифицированного сертификата путем использования стандартных атрибутов имени, описанные в справочнике выбранных типов атрибутов.[1] Для включения в квалифицированный сертификат информации о владельце квалифицированного сертификата, для которой не предусмотрены соответствующие стандартные атрибуты имени, по согласованию сторон может быть использовано дополнение subjectAlternativeName

[1] Выбранные типы атрибутов определены в ГОСТ Р ИСО/МЭК 9594-6-98 "Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 6. Выбранные типы атрибутов" и в международном стандарте КОЛЕС 9594-6:2008 "Information technology - Open systems interconnection - The Directory: Selected attribute types", опубликованном по адресу в информационно-телекоммуникационной сети Интернет: http://www.itu.int/rec/T-REC-X.520-200811-I/en.

9.2. Форма списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра
thisUpdate	Время издания	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки события, повлекшего прекращение или приостановление действия сертификата (Time) 3. Код причины прекращения действия сертификата (Reson Code) "0" Не указана "1" Компрометация ключа (нарушение конфиденциальности ключа) "2" Компрометация ЦС (нарушение конфиденциальности ключа Удостоверяющего центра) "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
signatureAlgorithm	Алгоритм электронной 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 ключа центра сертификации, которым подписан данный СОС
CRL Number	Порядковый номер	Некритическое рекомендуемое расширение, содержащее порядковый номер списка отозванных сертификатов
Next Publication	Время издания СОС	Дата и время следующей плановой публикации СОС
szOID_CERTSRV_CA_VERSION	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего Центра

9.3. Сроки действия ключевых документов

9.3.1. Сроки действия ключевых документов Удостоверяющего центра

Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени генерации ключа электронной подписи Удостоверяющего центра.

Срок действия сертификата ключа проверки электронной подписи Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

9.3.2. Сроки действия ключевых документов Оператора и Пользователя Удостоверяющего центра

Срок действия ключа электронной подписи Оператора и Пользователя Удостоверяющего центра составляет 1 (один) год.

Начало периода действия ключа электронной подписи Оператора и Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра не превышает 14 (четырнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Оператора и Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

Срок действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра составляет 1 (один) год. Время начала периода действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно

10. Дополнительные положения

10.1. Плановая смена ключей Удостоверяющего центра

Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется в период действия ключа электронной подписи Удостоверяющего центра.

Процедура плановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр создает новый сертификат ключа проверки электронной подписи.

Старый ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, создаваемых Удостоверяющим центром в период действия старого ключа электронной подписи Удостоверяющего центра.

10.2. Нарушение конфиденциальности ключевых документов Удостоверяющего центра, внеплановая смена ключей Удостоверяющего центра

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра прекращает действие, Пользователи Удостоверяющего центра уведомляются об указанном факте путем публикации информации о нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра на сайте Удостоверяющего центра. Все сертификаты, подписанные с использованием ключа Удостоверяющего центра, конфиденциальность которого нарушена, считаются прекратившими действие.

После прекращения действия сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется процедура внеплановой смены ключей Удостоверяющего центра. Процедура внеплановой смены ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра.

Все действовавшие на момент нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

10.3. Нарушение конфиденциальности ключевых документов Оператора Удостоверяющего центра

Оператор Удостоверяющего центра самостоятельно принимает решение о факте или угрозе нарушения конфиденциальности своего ключа электронной подписи.

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Оператор Удостоверяющего центра прекращает или приостанавливает действие сертификата, соответствующего ключу, конфиденциальность которого нарушена или находится под угрозой нарушения, посредством подачи соответствующего заявления согласно настоящему Регламенту.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Оператор Удостоверяющего центра не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр прекращает действие данного сертификата.

Выдача нового сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра осуществляется согласно п.8.2. Регламента.

10.4. Конфиденциальность информации

10.4.1. Типы конфиденциальной информации

10.4.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключей электронных подписей Операторов и Пользователей Удостоверяющего центра.

10.4.1.2. Персональная и корпоративная информация об Операторах и Пользователях Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

10.4.2. Типы информации, не являющейся конфиденциальной

10.4.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

10.4.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

10.4.2.3. Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

10.4.2.4. Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, создаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

10.4.2.5. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

10.4.3. Исключительные полномочия Удостоверяющего центра

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

10.5. Хранение сертификатов ключей проверки электронной подписи в Удостоверяющем центре

Срок хранения сертификата ключа проверки электронной подписи в Удостоверяющем центре осуществляется в течение всего периода его действия и 5 (Пять) лет после его прекращения действия. По истечении указанного срока хранения сертификаты ключей проверки электронной подписи переводятся в режим архивного хранения.

10.6. Прекращение оказания услуг Удостоверяющим центром

10.6.1. В случае прекращения действия настоящего Регламента в отношении Уполномоченной организации действие сертификатов ключей проверки электронной подписи Оператора Удостоверяющего центра, как представителя Уполномоченной организации, а также действие сертификатов ключей проверки электронной подписи, решение по созданию и выдаче которых принял Оператор Удостоверяющего центра, по усмотрению Удостоверяющего центра может быть прекращено.

10.7. Непреодолимая сила (форс-мажор)

10.7.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

10.7.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратнопрограммного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

10.7.3. В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

10.7.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

10.7.5. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

10.7.6. В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

11. Список приложений

11.1. Приложение №1-А. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с формированием ключей электронной подписи Администратором Удостоверяющего центра

11.2. Приложение №1-Б. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по Запросу на сертификат.

11.3. Приложение №2. Форма доверенности Оператора Удостоверяющего центра.

11.4. Приложение №3-А. Форма доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи за Оператора Удостоверяющего центра.

11.5. Приложение №3-Б. Форма доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи за Оператора Удостоверяющего центра.

11.6. Приложение №4. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

11.7. Приложение №5. Форма заявления на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

11.8. Приложение №6. Форма заявления на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра. 11.7.

11.10. Приложение №7. Форма заявления на проверку подлинности электронной подписи в электронном документе.

11.11. Приложение №8. Форма копии сертификата ключа проверки электронной подписи на бумажном носителе.

11.12. Приложение №9. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «Гвард-Информ» и, определяющих ограничения использования квалифицированного сертификата.

11.13. Приложение №10. Технические ограничения на длину полей сертификата.

11.14. Приложение №11. Обязанности Пользователя Удостоверяющего центра

11.15. Приложение №12. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Приложение №1-А
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с формированием ключей электронной подписи Администратором Удостоверяющего центра)

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с формированием ключей электронной подписи Администратором Удостоверяющего центра

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность, фамилия, имя, отчество)

действующего на основании _____

Просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронный подписи на предоставленный ключевой носитель.

В качестве владельца сертификата ключа проверки электронной подписи наряду с указанием в сертификате наименования нашей организации прошу указать следующего полномочного представителя, действующего от имени нашей организации – Оператора Удостоверяющего центра:

_____

(фамилия, имя, отчество полномочного представителя)

В сертификат ключа проверки электронной подписи прошу занести следующие идентификационные данные:

CommonName (CN)	Наименование организации или ФИО уполномоченного лица
INN	ИНН организации
OGRN	ОГРН организации
Organization (O)	Наименование организации
Locality (L)	Город
StreetAdrdess (STREET)	Улица, номер дома, корпуса, строения, помещения
State (S)	Субъект Российской Федерации
Contry (C)	Страна=RU
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество полномочного представителя
СНИЛС	Страховой номер индивидуального лицевого счета
Title (T)	Должность полномочного представителя (необязательное поле)
OrganizationUnit (OU)	Наименование подразделения полномочного представителя (необязательное поле)
E-Mail (E)	Адрес электронной почты полномочного представителя

и следующие ограничения использования квалифицированного сертификата:
□ Оператор удостоверяющего центра (OID 1.2.643.2.2.34.5).

Настоящим _____
(фамилия, имя, отчество полномочного представителя)
_____
(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой Удостоверяющим центром ООО «Гвард-Информ» своих персональных данных, указанных в предоставляемых копиях документа, удостоверяющего личность и страхового свидетельства обязательного (государственного) пенсионного страхования, а также в настоящем заявлении, с целью создания сертификата ключа проверки электронной подписи, а также исполнения иных функций, возложенных на Удостоверяющий центр ООО "Гвард-Информ" федеральным законом от 06.04.2011 N 63-ФЗ.

Оператор Удостоверяющего центра
ООО «Гвард-Информ» _____

«____» _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления Печать организации

Приложение №1-Б
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма заявления на создание квалифицированного сертификата
ключа проверки электронной подписи Оператора
Удостоверяющего центра по Запросу на сертификат)

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по Запросу на сертификат

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность, фамилия, имя, отчество)

действующего на основании _____

Просит создать сертификат ключа проверки электронный подписи согласно предоставленному Запросу на сертификат содержащему указанные ниже сведения, включая следующие ограничения:

«Оператор Удостоверяющего центра» (OID 1.2.643.2.2.34.5).

В качестве владельца сертификата ключа проверки электронной подписи наряду с указанием в сертификате наименования нашей организации прошу указать следующего полномочного представителя, действующего от имени нашей организации – Оператора Удостоверяющего центра:

_____

(фамилия, имя, отчество полномочного представителя)

Сведения о запросе на сертификат:

_____

Версия: 1
Субъект:
CN=ООО "Ромашка"
O=ООО "Ромашка"
SN=Иванов
G=Иван Иванович
T=Руководитель
СНИЛС=06861980104
ИНН=005101007322
ОГРН=1037556120337
E=5tgb56@inbox.ru
STREET=ул.Строителей, д.5
L=Тула
S=71 Тульская область
C=RU
Алгоритм открытого ключа:
ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001
Параметры алгоритма:
0000 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03

0010 02 02 1e 01
1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию
1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию
Длина открытого ключа: 512 бит
Открытый ключ: UnusedBits = 0
0000 04 40 4d 26 06 a9 6a b8 0c e3 f9 ea 8c 1d d7 58
0010 fa 5a 4b b6 c0 20 79 e0 be b2 13 45 55 1f eb e6
0020 47 ee f1 75 83 36 49 13 82 c2 ac 88 34 d3 cf f0
0030 b0 60 27 6b 21 b0 1c 8a 1c 24 ce 02 a4 28 4a ca
0040 e9 7b
Запрос атрибутов: 1
Атрибуты 1:
Атрибут[0]: 1.3.6.1.4.1.311.2.1.14 (Расширения сертификатов)
Значение[0][0]:
Неизвестный тип атрибута
Расширения сертификатов: 5
2.5.29.15: Флаги = 1(Критический), Длина = 4
Использование ключа
Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

2.5.29.37: Флаги = 0, Длина = 28
Улучшенный ключ
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)
Оператор Центра Регистрации (1.2.643.2.2.34.5)

Настоящим _____

(фамилия, имя, отчество полномочного представителя)

_____

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой Удостоверяющим центром ООО «Гвард-Информ» своих персональных данных, указанных в предоставляемых копиях документа, удостоверяющего личность и страхового свидетельства обязательного (государственного) пенсионного страхования, а также в настоящем заявлении, с целью создания сертификата ключа проверки электронной подписи, а также исполнения иных функций, возложенных на Удостоверяющий центр ООО "Гвард-Информ" федеральным законом от 06.04.2011 N 63-ФЗ.

Оператор Удостоверяющего центра
ООО «Гвард-Информ» _____

«____» _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления Печать организации

Приложение №2
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма доверенности Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

действовать от имени _____
(полное наименование организации)

при использовании электронной подписи электронных документов, выступать в роли Оператора Удостоверяющего центра ООО «Гвард-Информ» и осуществлять действия в рамках Регламента Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи (Схема обслуживания: с уполномоченной организацией), установленные для Оператора Удостоверяющего центра ООО «Гвард-Информ».

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

Подпись уполномоченного представителя _____ _____
(Фамилия И.О.) (Подпись)

подтверждаю.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №3-А
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи за Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

получить ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные для Оператора Удостоверяющего центра

_____
(фамилия, имя, отчество Пользователя Удостоверяющего центра)

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

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

Подпись уполномоченного представителя _____ _____
(Фамилия И.О.) (Подпись)

подтверждаю.

Оператор Удостоверяющего центра
ООО «Гвард-Информ» _____

«____» _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №3-Б
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма доверенности на получение сертификата ключа
проверки электронной подписи за Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

сертификат ключа проверки электронной подписи, созданный для Оператора Удостоверяющего центра

_____
(фамилия, имя, отчество Пользователя Удостоверяющего центра)

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

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

Подпись уполномоченного представителя _____ _____
(Фамилия И.О.) (Подпись)

подтверждаю.

Оператор Удостоверяющего центра
ООО «Гвард-Информ» _____

«____» _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №4
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма заявления на прекращение действия сертификата
ключа проверки электронной подписи)

Заявление на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____

Просит прекратить действие своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Наименование организации
INN	ИНН организации
OGRN	ОГРН организации
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество полномочного представителя

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №5
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма заявления на приостановление действия сертификата ключа проверки электронной подписи)

Заявление на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Наименование организации
INN	ИНН организации
OGRN	ОГРН организации
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество полномочного представителя

Срок приостановления действия сертификата _____ дней.
(количество прописью)

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления Печать организации

Приложение №6
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма заявления на возобновление действия сертификата
ключа проверки электронной подписи)

Заявление на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Наименование организации
INN	ИНН организации
OGRN	ОГРН организации
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество полномочного представителя

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления Печать организации

Приложение №7
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма заявления на проверку подлинности электронной
подписи в электронном документе)

Заявление на проверку подлинности электронной подписи в электронном документе

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность руководителя)

_____,

(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–ХХХ;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–ХХХ
3. Время[1] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»;

Час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

«_____:_____» «_____/_____/_____»;

Час минута день месяц год

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

[1] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени).

Приложение №8
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма сертификата ключа проверки электронной подписи на бумажном носителе)
(для Оператора и Клиентов Уполномоченной организации - юридических лиц)

Копия сертификата ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан: ООО «Рога и копыта»
Кем выдан:ООО "Гвард-Информ"
Действителен с 01 июля 2013 г. 14:33:00 UTC по 01 июля 2014 г. 14:43:00 UTC
Версия: 3 (0x2)
Серийный номер: 5446 C8D7 0000 0000 0002
Издатель сертификата: CN = ООО "Гвард-Информ", C = RU, S = 71 Тульская область, L = Тула, O = ООО "Гвард-Информ", STREET = пр-кт Ленина д. 46, ОГРН = 1027100971182
Срок действия:
Действителен с: 01 июля 2013 г. 14:33:00 UTC
Действителен по: 01 июля 2014 г. 14:43:00 UTC
Владелец сертификата: CN = ООО "Рога и копыта", SN = Иванов, G = Иван Иванович, C = RU, S = 71 Тульская область, L = Тула, STREET = ул. Ленина, д. 5, оф. 70, O = ООО «Рога и копыта», OU = Отдел снабжения, T = Начальник отдела, ОГРН = 1234567890123, СНИЛС=12345678901, ИНН = 1234567890
Ключ проверки электронной подписи:
Алгоритм ключа проверки электронной подписи:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 1B94 ABF7 05B1 FC40 E4C0 3FEF 4AEF 4FF9 4BC0 5EFF 3B6F D799 B0B6 F1F4 A934 B0B3 3BF2 4D91 8B85 75E0 23A0 4954 4A5B 62D6 1E9C 9E85 38FF 5AA7 9FB8 BC00 1965 E825
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.32
Название: Политики сертификата
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1 [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2
4. Расширение 1.2.643.100.111
Название: Средство электронной подписи владельца
Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6)
5.Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 81 4d 19 d4 bf a9 3e b1 04 82 5b 7f 27 6f e6 fd 24 63 14 8b
6. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=42 c7 6c ab 78 59 89 f3 a7 3d 90 d2 d1 14 fd 4c 4f 01 5c 25 Поставщик сертификата: Адрес каталога: CN=ООО "Гвард-Информ" C=RU S=71 Тульская область L=Тула O=ООО "Гвард-Информ" STREET=пр-кт Ленина д. 46 ОГРН=1027100971182 ИНН=007107065081 Серийный номер сертификата=6a 5d e9 bf fa f7 d6 8b 45 ba ae 5e 68 bd 93 82
7. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://qca.ginf.ru/cdp/42c76cab785989f3a83d90d2d114fd4c4f025c25.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://ginf-qca.ru/cdp/42c76cab785989f3a83d90d2d114fd4c4f025c25.crl

8. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://qca.ginf.ru/cacert/42c76cab785989f3a83d90d2d114fd4c4f025c25.cer [2]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://ginf-qca.ru/cacert/42c76cab785989f3a83d90d2d114fd4c4f025c25.cer
9. Расширение 2.5.29.16
Название: Период использования закрытого ключа
Значение: Действителен с 01 июля 2013 г. 18:33:00 Действителен по 1 июля 2014 г. 18:33:00
10. Расширение 1.2.643.100.112
Название: Средства электронной подписи и УЦ издателя
Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6) Заключение на средство ЭП: СФ/124-1543 от 04 октября 2010 г. Средство УЦ: "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 Заключение на средство УЦ: СФ/128-1658 от 01 мая 2011 г.
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: 970C B533 48F5 2174 2940 4757 4F43 821A 75FA 852E 6EA4 EBE2 E480 D276 1438 6CFA 3C8D 7D17 4841 39F8 B322 7412 7986 762A 5F07 EC3E 9C1E 8A78 EA0A E78E 5363 1D22

Уполномоченное лицо УЦ: _____/_____
Подпись владельца сертификата: _____/_____
"___" _____ 20__ г.
М. П.

Приложение №8
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Форма сертификата ключа проверки электронной подписи на бумажном носителе)
(для Клиентов Уполномоченной организации - физических лиц)

Копия сертификата ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан: Иванов Иван Иванович
Кем выдан:ООО "Гвард-Информ"
Действителен с 01 июля 2013 г. 14:33:00 UTC по 01 июля 2014 г. 14:43:00 UTC
Версия: 3 (0x2)
Серийный номер: 5446 C8D7 0000 0000 0002
Издатель сертификата: CN = ООО "Гвард-Информ", C = RU, S = 71 Тульская область, L = Тула, O = ООО "Гвард-Информ", STREET = пр-кт Ленина д. 46, ОГРН = 1027100971182
Срок действия:
Действителен с: 01 июля 2013 г. 14:33:00 UTC
Действителен по: 01 июля 2014 г. 14:43:00 UTC
Владелец сертификата: CN = Иванов Иван Иванович, SN = Иванов, G = Иван Иванович, C = RU, S = 71 Тульская область, L = Тула, STREET = ул. Ленина, д. 5, кв. 71, ОГРН = 1234567890123, СНИЛС=12345678901, ИНН = 1234567890
Ключ проверки электронной подписи:
Алгоритм ключа проверки электронной подписи:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 1B94 ABF7 05B1 FC40 E4C0 3FEF 4AEF 4FF9 4BC0 5EFF 3B6F D799 B0B6 F1F4 A934 B0B3 3BF2 4D91 8B85 75E0 23A0 4954 4A5B 62D6 1E9C 9E85 38FF 5AA7 9FB8 BC00 1965 E825
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.32
Название: Политики сертификата
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1 [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2
4. Расширение 1.2.643.100.111
Название: Средство электронной подписи владельца
Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6)
5.Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 81 4d 19 d4 bf a9 3e b1 04 82 5b 7f 27 6f e6 fd 24 63 14 8b
6. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=42 c7 6c ab 78 59 89 f3 a7 3d 90 d2 d1 14 fd 4c 4f 01 5c 25 Поставщик сертификата: Адрес каталога: CN=ООО "Гвард-Информ" C=RU S=71 Тульская область L=Тула O=ООО "Гвард-Информ" STREET=пр-кт Ленина д. 46 ОГРН=1027100971182 ИНН=007107065081 Серийный номер сертификата=6a 5d e9 bf fa f7 d6 8b 45 ba ae 5e 68 bd 93 82
7. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://qca.ginf.ru/cdp/42c76cab785989f3a83d90d2d114fd4c4f025c25.crl [2]Точка распределения списка

отзыва (CRL) Имя точки распространения: Полное имя: URL=http://ginf-qca.ru/cdp/42c76cab785989f3a83d90d2d114fd4c4f025c25.crl
8. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://qca.ginf.ru/cacert/42c76cab785989f3a83d90d2d114fd4c4f025c25.cer [2]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://ginf-qca.ru/cacert/42c76cab785989f3a83d90d2d114fd4c4f025c25.cer
9. Расширение 2.5.29.16
Название: Период использования закрытого ключа
Значение: Действителен с 1 июля 2013 г. 18:33:00 Действителен по 1 июля 2014 г. 18:33:00
10. Расширение 1.2.643.100.112
Название: Средства электронной подписи и УЦ издателя
Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6) Заключение на средство ЭП: СФ/124-1543 от 04 октября 2010 г. Средство УЦ: "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 Заключение на средство УЦ: СФ/128-1658 от 01 мая 2011 г.

Подпись Удостоверяющего центра:

Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: 970C B533 48F5 2174 2940 4757 4F43 821A 75FA 852E 6EA4 EBE2 E480 D276 1438 6CFA 3C8D 7D17 4841 39F8 B322 7412 7986 762A 5F07 EC3E 9C1E 8A78 EA0A E78E 5363 1D22

Уполномоченное лицо УЦ: _____/_____
Подпись владельца сертификата: _____/_____
"___" _____ 20__ г.
М. П.

Приложение №9
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «Гвард-Информ» и определяющих ограничения использования квалифицированного сертификата)

Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «Гвард-Информ» и определяющих ограничения использования квалифицированного сертификата.

№ п/п	OID	Наименование	Ограничение
1	1.2.643.3.91.3.1	Только для использования в системах сдачи отчетности	Сертификаты содержащие данное ограничение могут быть использованы только в рамках систем документооборота (в т.ч. сдачи отчетности) с ФНС, ПФР, Росстат и ФСС.
2	1.2.643.5.1.28.2	Только для использования в информационных системах Федеральной службы по регулированию алкогольного рынка	Сертификаты содержащие данное ограничение могут быть использованы только в рамках информационных систем Федеральной службы по регулированию алкогольного рынка
3	1.2.643.5.1.28.3	Только для использования в информационных системах Федеральной службы по регулированию алкогольного рынка	Сертификаты содержащие данное ограничение могут быть использованы только в рамках информационных систем Федеральной службы по регулированию алкогольного рынка
4	1.2.643.5.1.28.4	Только для использования в информационных системах Федеральной службы по регулированию алкогольного рынка	Сертификаты содержащие данное ограничение могут быть использованы только в рамках информационных систем Федеральной службы по регулированию алкогольного рынка
5	1.2.643.2.2.34.5	Оператор Удостоверяющего центра	Сертификаты содержащие данное ограничение могут быть использованы только для выполнения действий в качестве Оператора Удостоверяющего центра
6	1.2.643.3.91.4.1	Не для операций с недвижимостью либо заключения сделок.	Сертификаты содержащие данное ограничение не могут быть использованы: • для совершения каких-либо операций с недвижимостью; • для заключения каких-либо сделок;

Приложение №10
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Технические ограничения на длину полей сертификата)

Технические ограничения на длину полей сертификата.

Наименование поля сертификата	Описание поля	Максимальное количество символов, включая пробелы, шт.
(CN)	ФИО - для физического лица, Наименование ЮЛ или ФИО уполномоченного лица - для юридического лица	64
INN	ИНН	12
OGRN	ОГРН	13
(O)	Наименование организации	64
(L)	Город	128
(STREET)	Часть адреса места нахождения, включающую наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения.	30
(S)	Субъект Российской Федерации	128
(C)	Двухсимвольный код страны	2
(SN)	Фамилия	40
(GN)	Имя и Отчество	32
СНИЛС	Страховой номер индивидуального лицевого счета	11
(T)	Наименование должности лица (необязательное поле)	64
(OU)	Наименование подразделения юридического лица (необязательное поле)	64

Приложение №11
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Обязанности Пользователя Удостоверяющего центра)

Пользователь Удостоверяющего центра, являющийся Клиентом Уполномоченной организации, обязан:

1. Обеспечить конфиденциальность ключей электронных подписей.

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

3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

5. Немедленно обратиться в Уполномоченную организацию с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр (Уполномоченную организацию), в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр (Уполномоченную организацию) по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр (Уполномоченную организацию), в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр (Уполномоченную организацию) по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

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

9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

10. Уничтожить личный ключ электронной подписи в соответствии с эксплуатационной документацией на СКЗИ сразу по окончании срока его действия

Приложение №12
к Регламенту Удостоверяющего центра ООО «Гвард-Информ» по
созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: с уполномоченной организацией)
(Руководство по обеспечению безопасности использования
квалифицированной электронной подписи и средств
квалифицированной электронной подписи)

Пользователь обязан:

- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств квалифицированной электронной подписи;
- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих ему ключей электронных подписей без его письменного согласия;
- немедленно уведомлять работодателя о фактах утраты или недостачи средств квалифицированной электронной подписи, ключевых документов к ним и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;
- уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- использовать для создания и проверки, квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получавшие подтверждение соответствия требованиям, установленным в соответствии с действующим Федеральным законодательством;
- не использовать ключ электронной подписи и немедленно обратиться в удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если ограничения установлены);
- сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним работодателю в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;

Пользователю запрещается:

- оставлять без контроля вычислительные средства, на которых экспортируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;
- запрещается оставлять ключевой носитель и PIN-код доступа к нему без присмотра, а так же передавать ключевой носитель и PIN-код доступа к нему кому бы то ни было
- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

- использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- использовать нестандартные, изменённые или отладочные версии операционных систем (ОС);
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.
- обрабатывать на ПЭВМ, оснащенной средством квалифицированной электронной подписи, информацию, содержащую государственную тайну.
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средством квалифицированной подписи.

Пользователь несет ответственность за:

- обеспечение конфиденциальности ключей ЭП, в частности не допущение использования принадлежащих ему ключей ЭП без его письменного согласия;
- не уведомление УЦ, выдавшего сертификат ключа проверки ЭП, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течении не более чем одного рабочего дня со дня получения информации о таком нарушении;
- использование ключа ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Ознакомлен

_____(Ф.И.О., подпись)