УТВЕРЖДАЮ
Директор краевого государственного
автономного учреждения
«Информационно-технологический
центр Камчатского края»

_____Н.Е. Шарипов
«30» июня 2020 г.

РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
КРАЕВОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО УЧРЕЖДЕНИЯ «ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР КАМЧАТСКОГО КРАЯ»

Редакция № 5
Введен приказом №28/2-од от «30» июня 2020 г.

г. Петропавловск-Камчатский

СОДЕРЖАНИЕ

1. Сведения об Удостоверяющем центре

Краевое государственное автономное учреждение «Информационно-технологический центр Камчатского края» (КГАУ «Информационно-технологический центр»), в состав которого входит Удостоверяющий центр, зарегистрировано на территории Российской Федерации в городе Петропавловск-Камчатский.

Свидетельство о государственной регистрации юридического лица от 10 октября 2011 года серии 41 № 000513595 выдано Инспекцией Федеральной налоговой службы РФ по г. Петропавловску-Камчатскому, ОГРН 1114101005600.

Свидетельство о постановке на учет российской организации в налоговом органе по месту нахождения на территории Российской Федерации от 10 октября 2011 года серии 41 № 000508433 выдано Инспекцией Федеральной налоговой службы г. Петропавловску-Камчатскому, ИНН 4101147350, КПП 410101001.

Удостоверяющий Центр в качестве профессионального участника рынка услуг по созданию и управлению сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании:

- Свидетельства об аккредитации удостоверяющего центра № 792, выданного Минкомсвязи России 04.09.2017.
- Лицензии ЛСЗ №0009721 рег. №39 от 02 апреля 2020 г., выданной УФСБ РФ по Камчатскому краю на право осуществление работ, предусмотренных пунктами 12, 20, 21 25, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, являющихся приложением к Положению, утверждённому постановлением Правительства Российской федерации от 16 апреля 2012г. №313.

Реквизиты КГАУ «Информационно-технологический центр»:
Полное наименование: Краевое государственное автономное учреждение «Информационно-технологический центр Камчатского края»
Юридический адрес:
683902, г. Петропавловск-Камчатский, ул. Арсеньева, д. 23
Фактическое местонахождение:
683902, г. Петропавловск-Камчатский, ул. Арсеньева дом 23
Банковские реквизиты:
Банк: Дальневосточный филиал ПАО «РОСБАНК» г. Владивосток;
БИК 040507871; Р/сч 40603810446574000000.
ИНН/КПП 4101147350/410101001;
ОКПО 61443473;
ОКАТО 30401000000;
ОГРН 1114101005600
Контактные телефоны, факс, адрес электронной почты:
Тел.: +7 (4152) 25 11 00
Сайт: http://itc.kamgov.ru E-mail: uc@kamgov.ru.

2. Термины и определения

Аккредитованный Удостоверяющий центр - удостоверяющий центр, прошедший процедуру признания уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи».

Владелец сертификата ключа проверки подписи - физическое лицо, юридическое лицо или индивидуальный предприниматель, которому в соответствии с Федеральным Законом от 06.04.2011 года № 63-ФЗ «Об электронной подписи» и настоящим Регламентом выдан сертификат ключа проверки электронной подписи.

Доверенное лицо – представитель физического лица, юридического лица, индивидуального предпринимателя, действующий на основании надлежащим образом оформленной доверенности на передачу документов для получения сертификата и/или получение сертификата.

Заявитель – физическое лицо, юридическое лицо, индивидуальный предприниматель, обратившийся за получением сертификата ключа проверки электронной подписи или иных услуг в Удостоверяющий центр.

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Квалифицированная электронная подпись - электронная подпись, которая соответствует всем признакам квалифицированной электронной подписи, определенным в Федеральном законе от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Ключевая информация – ключ электронной подписи и ключ проверки электронной подписи, предназначенные для формирования (проверки) электронной подписи, действующие в течение определенного срока.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

Ключ электронной подписи (ключ ЭП) - 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.

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. 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.

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Неквалифицированная электронная подпись - электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи, определенным в Федеральном законе от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Рабочий день Удостоверяющего центра (далее - рабочий день) - промежуток времени с 9:00 до 18.00 с понедельника по четверг и с 9.00 до 17.00 в пятницу, перерыв с 12.00 до 12.48 (время Камчатское UTC+12), за исключением выходных дней (суббота, воскресенье) и нерабочих праздничных дней.

Прием документов в Удостоверяющем центре - промежуток времени с 9:00 до 16.00 с понедельника по четверг и с 9.00 до 15.00 в пятницу, перерыв с 12.00 до 12.48 (время Камчатское UTC+12), за исключением выходных дней (суббота, воскресенье) и нерабочих праздничных дней.

Сертификат ключа проверки электронной подписи (СКПЭП) - 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 (отозван).

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.

Средства электронной подписи (средства ЭП) - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

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

Удостоверяющий центр (УЦ) - подразделение краевого государственного автономного учреждения «Информационно-технологический центр Камчатского края», осуществляющее выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным Законом от 06.04.2011 года № 63-ФЗ «Об электронной подписи».

Уполномоченный представитель Заявителя (далее – Уполномоченный представитель) – физическое лицо, которое действует от имени Заявителя на основании учредительных документов или доверенности и которое указывается в сертификате в качестве владельца наряду с данными Заявителя.

Уполномоченный сотрудник Удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное

Удостоверяющим центром соответствующими полномочиями согласно его функциональным обязанностям и (или) приказу.

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

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.

Иные термины и понятия в настоящем Регламенте используются в значениях, определенных нормативными правовыми актами Российской Федерации.

3. Статус Регламента

3.1. Регламент Удостоверяющего центра КГАУ «Информационно-технологический центр», именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

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

3.3. 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.

3.4. Настоящий регламент распространяется в форме электронного документа по адресу http://itc.kamgov.ru/files/uc/accred_reglament.pdf.

4. Общие положения

4.1. Присоединение к Регламенту

4.1.1. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления Заявителем в Удостоверяющий центр Заявления о присоединении к Регламенту. Форма Заявления о присоединении к Регламенту для юридических лиц и индивидуальных предпринимателей приведена в Приложении №1 к настоящему Регламенту, для физических лиц - в Приложении №2 к настоящему Регламенту.

4.1.2. С момента регистрации Заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившемся к Регламенту и является Стороной Регламента.

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

4.1.4. После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, считаются вступившими в соответствующие договорные отношения на неопределённый срок.

4.2.Порядок расторжения договорных отношений

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

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

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

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

4.3. Изменение (дополнение) Регламента

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

4.3.2. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения

указанных изменений (дополнений) на сайте Удостоверяющего центра по адресу - http://itc.kamgov.ru/files/uc/accred_reglament.pdf

4.3.3. Все изменения (дополнения), 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 и дополнений в Регламенте на сайте Удостоверяющего центра по адресу - http://itc.kamgov.ru/files/uc/accred_reglament.pdf

4.3.4. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

4.3.5. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном п.4.2. настоящего Регламента.

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

4.4. Применение Регламента

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

4.4.2.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.

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

5 . Предоставление информации

5.1.Удостоверяющий центр 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 Сторона, присоединившаяся к Регламенту, может ознакомиться на официальном сайте Минкомсвязи России.

5.2.Удостоверяющий центр осуществляет свою деятельность в соответствии с лицензиями ФСБ России на право осуществления технического обслуживания шифровальных (криптографических) средств, распространения шифровальных (криптографических) средств, оказания услуг в области шифрования информации. С копиями указанных лицензий Сторона, присоединившаяся к Регламенту, может ознакомиться по следующему адресу в сети Интернет – http://itc.kamgov.ru/.

5.3.Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить Удостоверяющему центру следующий перечень документов, необходимых для подтверждения сведений, заносимых в сертификат (далее – Заявительные документы).

5.3.1 Для юридических лиц:

- надлежащим образом оформленное Заявление на создание сертификата ключа проверки электронной подписи (с указанием в качестве владельца сертификата ключа проверки электронной подписи уполномоченного представителя - по форме Приложения №3, без указания в качестве владельца сертификата ключа проверки электронной подписи физического лица - по форме Приложения №4);
- если сертификат изготавливается на имя Уполномоченного представителя: доверенность, подтверждающую полномочия Уполномоченного представителя, оформленную по форме Приложения №6 настоящего Регламента, подписанную руководителем или иным лицом, уполномоченным на это учредительными документами Заявителя - юридического лица и заверенную печатью Заявителя - юридического лица;
- заверенную надлежащим образом копию Приказа о назначении (принятии на работу) Уполномоченного представителя, подтверждающего настоящую должность Уполномоченного представителя;
- паспорт гражданина Российской Федерации, на чье имя изготавливается сертификат (реквизиты документа, удостоверяющего личность);

- страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;
- если документы для изготовления сертификата предоставляет и / или получает не Заявитель, а его Доверенное лицо: доверенность на предоставление документов и / или получение ключевого документа и сертификата за Заявителя, по форме Приложения №7, подписанную руководителем или иным лицом, уполномоченным на это учредительными документами Заявителя - юридического лица и заверенную печатью Заявителя - юридического лица, с одновременным предъявлением паспорта гражданина РФ Доверенным лицом;
- иные дополнительные документы по усмотрению Удостоверяющего центра.

5.3.2 Для индивидуальных предпринимателей, имеющих печать:

- Основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП);
- идентификационный номер налогоплательщика;
- надлежащим образом оформленное Заявление на создание сертификата ключа проверки электронной подписи (по форме Приложения №3);
- заверенную надлежащим образом копию Приказа о назначении (принятии на работу) Уполномоченного представителя, подтверждающего настоящую должность Уполномоченного представителя;
- паспорт гражданина Российской Федерации, на чье имя изготавливается сертификат (реквизиты документа, удостоверяющего личность Владельца сертификата);
- страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;
- если документы для изготовления сертификата предоставляет и / или получает не Заявитель, а его Доверенное лицо: нотариально заверенную доверенность на предоставление документов и / или получение ключевого документа и сертификата за Заявителя, с одновременным предъявлением паспорта гражданина РФ Доверенным лицом;
- иные дополнительные документы по усмотрению Удостоверяющего центра.

5.3.3 Для индивидуальных предпринимателей, не имеющих печать:

- Основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП);

- идентификационный номер налогоплательщика;
- надлежащим образом оформленное Заявление на создание сертификата ключа проверки электронной подписи (по форме Приложения №3);
- паспорт гражданина Российской Федерации, на чье имя изготавливается сертификат (реквизиты документа, удостоверяющего личность Владельца сертификата);
- страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;
- если документы для изготовления сертификата предоставляет и / или получает не Заявитель, а его Доверенное лицо: нотариально заверенную доверенность на предоставление документов и / или получение ключевого документа и сертификата за Заявителя, с одновременным предъявлением паспорта гражданина РФ Доверенным лицом;
- иные дополнительные документы по усмотрению Удостоверяющего центра.

5.3.4 Для физических лиц:

- идентификационный номер налогоплательщика;
- надлежащим образом оформленное Заявление на создание сертификата ключа проверки электронной подписи (по форме Приложения №5);
- паспорт гражданина Российской Федерации (реквизиты документа, удостоверяющего личность Владельца сертификата);
- страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;
- если документы для изготовления сертификата предоставляет и / или получает не Заявитель, а его Доверенное лицо: нотариально заверенную доверенность на предоставление документов и / или получение ключевого документа и сертификата за Заявителя, с предъявлением паспорта гражданина РФ Доверенным лицом;
- иные дополнительные документы по усмотрению Удостоверяющего центра.

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

- для юридических лиц – заверенные нотариусом или лицом, действующим от имени юридического лица без доверенности и печатью юридического лица; заверение копий документов возможно работником - специалистом юридического лица, осуществляющим сопровождение кадровой работы с подтверждением указанных полномочий (заверенная копия должностной

инструкции (регламента), заверенная копия выписки из должностной инструкции (регламента));

- для индивидуальных предпринимателей, имеющих печать – заверенные нотариусом или уполномоченным сотрудником Удостоверяющего центра при условии предъявления оригиналов Заявительных документов, который сверяются с копиями и возвращаются Заявителю;
- для индивидуальных предпринимателей, не имеющих печать / физических лиц - заверенные нотариусом или уполномоченным сотрудником Удостоверяющего центра при условии предъявления оригиналов Заявительных документов, который сверяются с копиями и возвращаются Заявителю.

5.5.Сторона, присоединившаяся к Регламенту, несет ответственность за достоверность предоставленных в Удостоверяющий центр сведений.

5.6.Копии документов, подтверждающие сведения, внесенные в сертификат, подлежат хранению в соответствии с п. 12.7 раздела 12 настоящего Регламента.

6. Права и обязанности сторон

6.1. Удостоверяющий центр обязан:

6.1.1. Создать по обращению Стороны, присоединившейся к Регламенту, сертификат в соответствии с порядком, определенным в настоящем Регламенте, и предоставить Владельцу сертификат в электронной форме.

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

6.1.3. Обеспечить формирование ключей электронных подписей на отчуждаемых ключевых носителях, сертифицированных по требованиям безопасности информации в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей. При генерации и записи на ключевой носитель контейнера ключа электронной подписи исключать возможность его дублирования и экспорта.

6.1.4. Использовать ключ Удостоверяющего центра только для подписи издаваемых им сертификатов ключей проверки электронных подписей и списков отозванных сертификатов.

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

6.1.6. Организовать свою работу по Камчатскому времени. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

6.1.7. Информировать в письменной форме Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

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

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

6.1.8. Организовать ведение Реестра сертификатов, в том числе включающего в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращения или аннулирования.

6.1.9. Обеспечить актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

6.1.10. Предоставлять безвозмездно любому лицу по его обращению в соответствии с п. 10.3 настоящего Регламента информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании сертификата.

6.1.11. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки электронных подписей.

6.1.12. Обеспечить уникальность значений ключей проверки электронной подписи в изготовленных сертификатах ключей проверки электронных подписей Пользователей Удостоверяющего центра.

6.1.13. Обеспечить уникальность значений ключей проверки электронной подписи в созданных Удостоверяющим центром сертификатах.

6.1.14. Установить сроки действия сертификатов.

6.1.15. При получении сертификата ознакомить Владельца сертификата под расписку с информацией, содержащейся в сертификате.

6.1.16. Аннулировать сертификат, созданный в Удостоверяющем центре в случаях, указанных в пп. 10.2.1 п. 10.2 настоящего Регламента и порядке, определенном пп. 10.2.2 - 10.2.9 п. 10.2 настоящего Регламента.

6.1.17. Внести информацию об аннулировании сертификата в Реестр сертификатов с указанием даты и времени занесения и причины отзыва в течение 30 (тридцати) минут рабочего дня с момента уведомления уполномоченного лица Удостоверяющего центра о наступлении событий, указанных в п.6.1.16 настоящего Регламента, путем внесения соответствующей записи в Реестр сертификатов, а также опубликовать обновленный актуальный список аннулированных сертификатов в точках распространения списков аннулированных сертификатов.

6.1.18. Официально уведомить об аннулировании сертификата, созданного Удостоверяющим центром, посредством публикации списка аннулированных сертификатов.

6.1.19. Публиковать актуальные списки аннулированных сертификатов не реже 2 (двух) раз в сутки в точках распространения списков аннулированных сертификатов. Точки распространения списков аннулированных сертификатов указаны в сертификатах, находящихся в Реестре сертификатов.

6.1.20. Обеспечивать круглосуточную доступность списков аннулированных сертификатов в точках распространения списков аннулированных сертификатов.

6.1.21. Обеспечить оказание своевременной технической помощи Владельцам сертификатов по вопросам применения электронной подписи и средств электронной подписи.
6.1.22. Обеспечить круглосуточный прием заявок на оказание технической поддержки посредством направления заявок по адресу электронной почты: uc@kamgov.ru. При этом время реагирования сотрудников службы технической поддержки Удостоверяющего центра на запрос по вопросам технической поддержки не должно превышать 2 (двух) часов рабочего дня с момента поступления запроса в Удостоверяющий центр.

6.2. Сторона, присоединившаяся к Регламенту, обязана:
6.2.1. Известить Удостоверяющий центр об изменениях в Заявительных документах, и по требованию Удостоверяющего центра предоставить их в течение 5 (пяти) рабочих дней с даты регистрации изменений.
6.2.2. С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в 7 (семь) календарных дней обращаться на сайт Удостоверяющего центра по адресу http://itc.kamgov.ru/files/uc/accred_reglament.pdf за сведениями об изменениях и дополнениях в Регламент.

6.3. Владелец сертификата обязан:
6.3.1. Хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования, в частности не допускать использование принадлежащих ему ключей электронных подписей без его согласия.
6.3.2. Уведомить Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем 1 (одного) рабочего дня со дня получения информации о таком нарушении.
6.3.3. Применять для формирования электронной подписи только действующий ключ электронной подписи.
6.3.4. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
6.3.5. 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.

6.3.6. Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование сертификата ключа проверки электронной подписи, в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
6.3.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование, которого подано в Удостоверяющий центр в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата в Удостоверяющий центр по момент времени официального уведомления об аннулировании сертификата, либо об отказе в аннулировании.
6.3.8. Использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
6.3.9. Для хранения ключа электронной подписи применять ключевой носитель, поддерживаемый средством электронной подписи Удостоверяющего центра.

6.4. Удостоверяющий центр имеет право:
6.4.1. Отказать Стороне, присоединившейся к Регламенту, в создании сертификата и ключа электронной подписи в случае ненадлежащего оформления и/или непредоставления, а равно предоставления неполного комплекта Заявительных документов.
6.4.2. Отказать Стороне, присоединившейся к Регламенту, в создании сертификата и ключа электронной подписи в случае предоставления недостоверных сведений.
6.4.3. Отказать Стороне, присоединившейся к Регламенту, в создании сертификата и ключа электронной подписи в случае если услуга по созданию и выдаче сертификата не оплачена в надлежащем порядке.
6.4.4. Отказать в аннулировании сертификата, созданного Удостоверяющим центром, в случае ненадлежащего оформления соответствующего Заявления на аннулирование сертификата.
6.4.5. Отказать в аннулировании сертификата, созданного Удостоверяющим центром, в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату.
6.4.6. В одностороннем порядке аннулировать сертификат, созданный Удостоверяющим центром, с обязательным уведомлением Владельца сертификата, действие которого аннулировано, и указанием обоснованных причин.

6.4.7. Предоставлять сертификаты, содержащиеся в Реестре сертификатов, в электронной форме по запросу лица, обратившегося в Удостоверяющий Центр.

6.5. Владелец сертификата имеет право:

6.5.1. Получить сертификат ключа проверки электронной подписи Удостоверяющего центра.

6.5.2. Использовать сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в сертификатах, созданных Удостоверяющим центром.

6.5.3. Использовать список аннулированных сертификатов, созданный Удостоверяющим центром, для установления статуса сертификатов, созданных Удостоверяющим центром.

6.5.4. Получить Копию сертификата.

6.5.5. Обратиться в Удостоверяющий центр для аннулирования сертификата в течение срока действия соответствующего ему ключа электронной подписи.

7. Вознаграждение Удостоверяющего центра

7.1. Удостоверяющий Центр осуществляет свою деятельность на платной основе.

7.2. Стоимость, сроки и порядок расчетов за предоставляемые услуги Удостоверяющего центра регулируются договором между Удостоверяющим центром и Заявителем.

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

7.4. Создание сертификатов в связи с внеплановой сменой ключей Владельцев сертификатов, связанной с нарушением конфиденциальности ключей электронной подписи Удостоверяющего центра, осуществляется Удостоверяющим центром безвозмездно.

7.5. Удостоверяющий центр выполняет аннулирование сертификатов, содержащихся в Реестре сертификатов безвозмездно.

8. Ответственность сторон

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

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

8.3. Удостоверяющий центр 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 документах, предоставленных в соответствии с п.5.3 настоящего Регламента.

8.4. 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.

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

9. Разрешение споров

9.1. С Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к Регламенту.
9.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.
9.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.
9.4. Сторона, получившая от другой Стороны претензию, обязана в течение 30 (тридцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.
9.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в порядке, установленном действующим законодательством Российской Федерации.

10. Порядок предоставления и пользования услугами Удостоверяющего центра

10.1. Создание сертификата ключа проверки электронной подписи и сертификата

10.1.1. Удостоверяющий центр осуществляет регистрацию Заявителя в Удостоверяющем центре и изготовление ключей электронной подписи только в том случае, если Заявитель присоединился к Регламенту, в соответствии с п. 4.1 настоящего Регламента, а также при соблюдении Заявителем финансовых и других условий соответствующего договора.

10.1.2. Под регистрацией Заявителя в Удостоверяющем центре понимается внесение регистрационной информации о нем в реестр Удостоверяющего центра.

10.1.3. Процедура регистрации применяется в отношении лиц, обращающихся к услугам Удостоверяющего центра в части создания сертификатов и/или формирования ключей электронной подписи и ключей проверки электронной подписи с записью их на ключевой носитель.

10.1.4. Регистрация Заявителя, создание ключей электронной подписи и сертификата в Удостоверяющем центре осуществляется на основании Заявления на создание сертификата ключа проверки электронной подписи.

10.1.5. Заявление на создание сертификата ключа проверки электронной подписи должно содержать информацию, установленную статьей 17 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Вышеуказанное заявление должно предоставляться в Удостоверяющий центр вместе с Заявительными документами, которые подтверждают данные, заносимые в сертификат. Дополнительно (определяется Заявителем по согласованию с Удостоверяющим центром) заявление может содержать иную идентифицирующую Заявителя информацию.

10.1.6. Форма Заявления на создание сертификата ключа проверки электронной подписи для юридических лиц, индивидуальных предпринимателей приведена в Приложении №3 (с указанием в качестве владельца сертификата ключа проверки электронной подписи уполномоченного представителя) и Приложении №4 (без указания в качестве владельца сертификата ключа проверки электронной подписи физического лица) настоящего Регламента, для физических лиц - в Приложении №5 настоящего Регламента.

10.1.7. В случае создания сертификата юридическому лицу наряду с указанием в сертификате наименования юридического лица должно указываться физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Указанная доверенность должна предоставляться Заявителем вместе с Заявлением на создание сертификата ключа проверки электронной подписи, оформляться по форме

Приложения №6 настоящего Регламента и быть действительной на весь период использования ключа электронной подписи.

10.1.8. Если ключи электронной подписи и сертификат юридического лица будут использоваться для автоматического создания электронных подписей при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, то физическое лицо может не указываться в сертификате. Форма Заявления на создание сертификата ключа проверки электронной подписи для автоматического создания электронных подписей приведена в Приложении № 4 настоящего Регламента.

10.1.9. Предоставление Заявительных документов и/или получение созданных Удостоверяющим центром ключа электронной подписи и сертификата может быть осуществлено: для юридического лица / индивидуального предпринимателя:

- физическим лицом, которое указывается в сертификате наряду с наименованием юридического лица;
- физическим лицом на основании доверенности на получение ключей электронной подписи и сертификата, оформленной по форме Приложения №7 к настоящему Регламенту.

для физического лица:

- непосредственно указанным физическим лицом;
- физическим лицом на основании нотариально заверенной доверенности на получение ключей электронной подписи и сертификата, оформленной по форме Приложения № 8 к настоящему Регламенту.

10.1.10. При предоставлении Заявителем Заявительных документов Уполномоченный сотрудник Удостоверяющего центра выполняет процедуру идентификации Доверенного лица путем установления личности по паспорту или иному документу, удостоверяющему личность.

10.1.11. После положительной идентификации Доверенного лица Уполномоченный сотрудник Удостоверяющего центра принимает Заявительные документы, осуществляет их рассмотрение и принятие по ним решения.

10.1.12. В процессе рассмотрения Заявительных документов Уполномоченным сотрудником Удостоверяющего центра проверяется: корректность оформления заявлений и доверенностей; полнота комплекта заявительных документов; достоверность сведений в заявительных документах; правильность заверения копий заявительных документов. В ходе проверки достоверности сведений, указанных в Заявительных документах, Уполномоченный сотрудник Удостоверяющего центра устанавливает:

- факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно представляет;

- факт отсутствия явных признаков подделки документов.

10.1.13. Общее время рассмотрения Уполномоченным сотрудником Удостоверяющего центра Заявительных документов может быть не более 4 (четырех) часов с момента их поступления в Удостоверяющий центр в течение рабочего дня.

10.1.14. Уполномоченный сотрудник Удостоверяющего центра вправе отказать в изготовлении ключа электронной подписи и сертификата в следующих случаях:

- представления ненадлежащим образом оформленных Заявительных документов;
- противоречия сведений, указанных в Заявительных документах;
- не предоставления необходимого комплекта Заявительных документов;
- выявления факта подачи Заявительных документов с нарушением требований настоящего Регламента;
- необоснованного запроса полномочий;
- нарушения условий заключенного Договора на оказание услуг Удостоверяющего центра.

10.1.15. В случае обнаружения несоответствия данных, указанных в Заявительных документах, Уполномоченный сотрудник Удостоверяющего центра отказывает в изготовлении сертификата и возвращает Заявительные документы Заявителю (либо его Доверенному лицу) с указанием причины отказа.

10.1.16. По требованию лица, которому было отказано в изготовлении ключа электронной подписи и сертификата, Удостоверяющий центр предоставляет указанному лицу в день его обращения письменное мотивированное решение об отказе, заверенное подписью руководителя Удостоверяющего центра и печатью организации.

10.1.17.В случае принятия положительного решения Уполномоченный сотрудник Удостоверяющего центра на основе предоставленного Заявления на создание сертификата ключа проверки электронной подписи выполняет действия по созданию ключа электронной подписи и сертификата.

10.1.18. Ключ электронной подписи и сертификат записываются на ключевой носитель, предназначенный для хранения ключевой информации. Ключевой носитель может быть предоставлен Заявителем (его Доверенным лицом) или приобретен в Удостоверяющем центре.

10.1.19. Создание ключей электронных подписей осуществляется средством электронной подписи непосредственно на ключевой носитель, без сохранения сформированной ключевой информации Удостоверяющим центром на каком-либо ином носителе.

10.1.20. Создание и выдача ключа электронной подписи и сертификата осуществляется в день прибытия Заявителя или его доверенного лица в

Удостоверяющий центр. Дата прибытия Заявителя или его доверенного лица должна быть согласована с ответственным сотрудником Удостоверяющего центра.

10.1.21. Уполномоченный сотрудник Удостоверяющего центра изготавливает две копии сертификата на бумажном носителе по установленной форме согласно Приложению №13 (для юридических лиц и индивидуальных предпринимателей) или Приложению №14 (для физических лиц) к настоящему Регламенту. Все копии сертификата заверяются собственноручной подписью Заявителя или его Доверенного лица, а также собственноручной подписью ответственного лица Удостоверяющего центра, уполномоченного на осуществление указанного действия, а также печатью Удостоверяющего центра. Один экземпляр копии сертификата передается Заявителю, второй экземпляр подлежит архивному хранению в Удостоверяющем центре.

10.1.22. По окончании процедуры создания сертификата Заявителю или его Доверенному лицу выдаются:

- ключевой носитель, содержащий ключ электронной подписи и сертификат в электронной форме, соответствующий ключу электронной подписи;
- копия сертификата;
- руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи по форме Приложения №15 настоящего Регламента.

10.1.23. Выдача ключа электронной подписи и сертификата Заявителю (его Доверенному лицу) осуществляется под роспись в журнале поэкземплярного учета ключевых документов.

10.2 Аннулирование сертификата

10.2.1. Удостоверяющий центр аннулирует сертификат Владельца сертификата в следующих случаях:

- в случае прекращения действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту;
- в случае расторжения Договора на оказание услуг по созданию сертификата в связи с неисполнения или ненадлежащим исполнением обязательств по Договору;
- в случаях, предусмотренных Договором на оказание услуг по созданию сертификата;
- по истечении срока действия сертификата;
- по заявлению Владельца сертификата;
- в связи с вступлением в законную силу решения суда, повлекшего за собой аннулирование сертификата;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат;

- в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам.

10.2.2. Для аннулирования сертификата Владелец сертификата лично подает в Удостоверяющий центр заверенное собственноручной подписью надлежаще оформленное Заявление на аннулирование сертификата ключа проверки электронной подписи, либо в согласованном с Удостоверяющим центром порядке направляет такое заявление, подписанное действующей электронной подписью, в адрес Удостоверяющего центра в электронном виде по адресу электронной почты: uc@kamgov.ru.

10.2.3. Форма заявления на аннулирование сертификата ключа проверки электронной подписи приведена в Приложении № 9 (для юридических лиц и индивидуальных предпринимателей) и в Приложении №10 (для физических лиц) к настоящему Регламенту.

10.2.4. Время аннулирования сертификата и официального уведомления об этом Владельца данного сертификата, либо уведомления об отказе в аннулировании сертификата не должно превышать 30 (тридцати) минут рабочего дня с момента поступления в Удостоверяющий центр надлежаще оформленного Заявления, либо с момента вступившего в законную силу соответствующего судебного акта, либо с момента поступления сведений о других основаниях аннулирования сертификата.

10.2.5. Официальным уведомлением о факте аннулирования сертификата является опубликование списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате, и публикация обновленного актуального списка аннулированных сертификатов в точках распространения списков аннулированных сертификатов.

10.2.6. Аннулирование сертификата выполняется ответственным сотрудником Удостоверяющего центра, уполномоченным на совершение данного действия.

10.2.7. Временем аннулирования сертификата признается время внесения записи о его аннулировании в реестр сертификатов.

10.2.8. В случае аннулирования сертификата по истечении срока его действия временем его аннулирования признается время, хранящееся в поле notAfter поля Validity данного сертификата.

10.2.9. Информация о размещении списка аннулированных сертификатов заносится в созданные Удостоверяющим центром сертификаты в расширение CRL Distribution Poit.

10.3. Предоставление информации из Реестра сертификатов Удостоверяющего центра

10.3.1. Представление сертификата, находящегося в Реестре сертификатов, осуществляется на основании запроса в свободной форме с указанием информации, позволяющей идентифицировать сертификат в Реестре

сертификатов, и цели, для достижения которой должен быть представлен сертификат.

10.3.2. Сертификат представляется в форме электронного документа.

10.3.3. Срок предоставления Удостоверяющим центром сертификата из Реестра сертификатов не превышает 3 (трех) рабочих дней.

10.4. Подтверждение подлинности электронной подписи в электронном документе

10.4.1. По желанию Стороны, присоединившейся к Регламенту, Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению подлинности электронной подписи в электронном документе.

10.4.2. 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.

10.4.3. Для подтверждения подлинности электронной подписи в электронных документах Сторона, присоединившаяся к Регламенту, подает заявление в Удостоверяющий центр по форме Приложения №11 (для юридических лиц и индивидуальных предпринимателей) или Приложения №12 (для физических лиц) настоящего Регламента.

10.4.4. Обязательным приложением к Заявлению на подтверждение подлинности электронной подписи в электронном документе является usb-носитель, содержащий: • сертификат ключа проверки электронной подписи, с использованием которого необходимо подтвердить 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 (стандарта CMS).

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

10.4.6. Срок проведения работ по подтверждению подлинности электронной подписи в 1 (одном) электронном документе составляет 15 (пятнадцать) рабочих дней с момента поступления соответствующего заявления в Удостоверяющий центр и при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

10.4.7. При проведении работ по подтверждению подлинности электронной подписи Удостоверяющим центром может быть запрошена дополнительная информация.

10.4.8. Результатом проведения работ по подтверждению подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра, в котором обязательно содержится:

- состав комиссии Удостоверяющего центра, проводившей работы по подтверждению подлинности электронной подписи в электронном документе;
- основание для проведения работы по подтверждению подлинности;
- данные, представленные комиссии для проведения работ по подтверждению подлинности;
- результат проведения работы по подтверждению подлинности электронной подписи в электронном документе.

10.4.9. Заключение Удостоверяющего центра о результатах проведения работ по подтверждению подлинности электронной подписи в электронном документе составляется в произвольной форме в 2 (двух) экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения предоставляется Заявителю.

10.4.10. 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 Стороной, присоединившейся к Регламенту. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов, сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором.

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

11.1. Требования к структуре сертификатов, создаваемых Удостоверяющим центром

11.1.1. Сертификат должен соответствовать требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Приказом ФСБ РФ от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи», рекомендациями (разъяснениями) уполномоченных государственных органов.

11.1.2. Дополнительно в создаваемые Удостоверяющим центром сертификаты может быть занесено:

- в поле Subject (идентифицирует владельца сертификата):
  - ✓ Поле E (Email) - адрес электронной почты владельца сертификата;
  - ✓ Поле T (Title) - должность уполномоченного представителя (если владелец сертификата - юридическое лицо/индивидуальный предприниматель);
  - ✓ Поле SNILS – страховой номер индивидуального лицевого счета (СНИЛС) уполномоченного представителя (если владелец сертификата - юридическое лицо/индивидуальный предприниматель);
- расширение Private Key Validity Period - срок действия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи, следующего формата:
- Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;
- Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;
- расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) -набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с квалифицированным 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 поля и расширения по усмотрению Удостоверяющего центра.

11.1.3. Все поля и дополнения, включаемые в сертификаты, заполняются в соответствии с рекомендациями X.509 версии 3.

11.2. Структура идентификационных данных (структура поля Issuer) Удостоверяющего центра

Наименование поля	Описание	Содержание (значение)
Common Name, CN	Общее имя	УЦ ИТЦ КК
Organization Unit, OU	Подразделение	Удостоверяющий центр
Organization Name, O	Организация	КГАУ «Информационно-технологический центр Камчатского края»
Locality, L	Регион	41 Камчатский край
State, S	Населенный пункт	Петропавловск-Камчатский
Street	Название улицы, номер дома	улица Арсеньева дом 23
INN	ИНН	004101147350
OGRN	ОГРН	1114101005600

11.3. Требования к списку аннулированных сертификатов Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра (п.11.2 настоящего Регламента)
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1.Серийный номер сертификата (CertificateSerialNumber) 2.Время обработки события, повлекшего прекращение или приостановлени действия сертификата (Time) 3. Код причины прекращения действия сертификата (Reason 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 "6" Приостановление действи
signatureAlgorithm	Алгоритм электронной подписи	ГОСТ Р 34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.10-2012
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Удостоверяющего Центра
CRL Number	Порядковый номер CRL	Цифровое значение

11.4.Срок действия ключевых документов Удостоверяющего центра

11.4.1. Срок действия ключа электронной подписи Удостоверяющего центра составляет 3 (три) года.

11.4.2. Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени создания ключа электронной подписи Удостоверяющего центра.
11.4.3. Общее время использования ключа электронной подписи Удостоверяющего центра для выполнения целевых функций в течение трёх лет его действия ограничено 1 годом и 3 месяцами (остальное время ключ электронной подписи Удостоверяющего центра используется только для подписания списков аннулированных сертификатов).
11.4.4. Срок действия сертификата ключа проверки электронной подписи Удостоверяющего центра составляет 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.

11.5.Сроки действия ключевых документов Владельцев сертификатов

11.5.1. Срок действия ключа электронной подписи Владельца сертификата составляет не более 15 месяцев.
11.5.2. Начало периода действия ключа электронной подписи Владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата.
11.5.3. Срок действия сертификата Владельца сертификата составляет не более 15 месяцев.
11.5.4. Время начала периода действия сертификата Владельца сертификата и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

12. Дополнительные положения

12.1. Плановая смена ключевых документов Удостоверяющего центра

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

12.1.2. Процедура плановой смены ключей Удостоверяющего центра определяется эксплуатационной документацией на средства Удостоверяющего центра.

12.1.3. Уведомление пользователей о проведении смены ключей Удостоверяющего центра осуществляется посредством размещения сведений на сайте Удостоверяющего центра http://itc.kamgov.ru.

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

12.2. Внеплановая смена ключевых документов Удостоверяющего центра

12.2.1. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра аннулируется, Владельцы сертификатов уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте, указанной в Заявлении на создание сертификата ключа проверки электронной подписи, и публикации информации о нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра на сайте Удостоверяющего центра по адресу: http://itc.kamgov.ru. Все сертификаты, подписанные с использованием ключа электронной подписи Удостоверяющего центра, конфиденциальность которого нарушена, считаются прекратившими действие.

12.2.2. После аннулирования 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 (п. 12.1 настоящего Регламента).

12.2.3. Все подписанные с использованием ключа электронной подписи Удостоверяющего центра, конфиденциальность которого была нарушена, и действовавшие на момент нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификаты подлежат внеплановой смене.

12.3 Нарушение конфиденциальности ключевых документов Владельца сертификата

12.3.1. Владелец сертификата самостоятельно принимает решение о факте или угрозе нарушения конфиденциальности ключа электронной подписи.

12.3.2. В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Владелец сертификата связывается с Удостоверяющим центром и передает заполненное заявление на аннулирование сертификата, соответствующего скомпрометированному ключу.

12.4 Конфиденциальность информации

12.4.1. Типы конфиденциальной информации

Ключ электронной подписи является конфиденциальной информацией лица, являющегося Владельцем соответствующего сертификата. Удостоверяющий центр не осуществляет хранение ключей электронной подписи Владельцев сертификатов.

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

12.4.2. Типы информации, не являющейся конфиденциальной

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

Информация, включаемая в сертификаты и списки аннулированных сертификатов, создаваемые Удостоверяющим центром, не считается конфиденциальной.

Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, создаваемые Удостоверяющим центром, относятся к общедоступным персональным данным. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

12.5. Исключительные полномочия Удостоверяющего центра

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

12.6. Хранение сертификатов в Удостоверяющем центре

Хранение сертификата в Удостоверяющем центре осуществляется в течение всего срока деятельности Удостоверяющего центра.

12.7 Требования к документальному фонду Удостоверяющего центра

12.7.1. Хранение документального фонда Удостоверяющего центра (в том числе Заявительных документов, послуживших основанием для внесения сведений в сертификат) должно быть организовано в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

12.7.2. Копии Заявительных документов на бумажных носителях с резолюциями ответственных за выпуск сертификатов лиц Удостоверяющего центра, подлежат хранению в архивохранилище в течение всего срока деятельности Удостоверяющего центра.

12.7.3. Удостоверяющий центр обязан в течение всего срока своей деятельности хранить следующую информацию:

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

12.8. Прекращение оказания услуг Удостоверяющим центром

В случае расторжения Регламента по инициативе одной из Сторон все сертификаты, владельцем которых является Сторона, присоединившаяся к Регламенту, аннулируются Удостоверяющим центром.

12.9. Непреодолимая сила (форс-мажор)

12.9.1. 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.

12.9.2. 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 аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

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

12.9.4. 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.

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

12.9.6. 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.

Приложение

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

2. Приложение №2. Форма заявления о присоединении к Регламенту Удостоверяющего центра для физических лиц.

3. Приложение №3. Форма заявления на создание сертификата ключа проверки электронной подписи для юридических лиц и индивидуальных предпринимателей.

4. Приложение №4. Форма заявления на создание сертификата ключа проверки электронной подписи для юридических лиц без указания физического лица (для автоматического создания электронных подписей).

5. Приложение №5. Форма заявления на создание сертификата ключа проверки электронной подписи для физических лиц.

6. Приложение №6. Форма доверенности Удостоверяющего центра.

7. Приложение №7. Форма доверенности на получение ключевого (-ых) документа (-ов), сертификата (-ов) ключа (-ей) проверки электронной подписи за Владельца (-ев) сертификата в Удостоверяющем центре КГАУ «ИТЦ Камчатского края» для юридических лиц и индивидуальных предпринимателей.

8. Приложение №8. Форма доверенности на получение ключевого (-ых) документа (-ов), сертификата (-ов) ключа (-ей) проверки электронной подписи за Владельца (-ев) сертификата в Удостоверяющем центре КГАУ «ИТЦ Камчатского края» для физических лиц.

9. Приложение №9. Форма заявления на аннулирование сертификата ключа проверки электронной подписи для юридических лиц и индивидуальных предпринимателей.

10. Приложение №10. Форма заявления на аннулирование сертификата ключа проверки электронной подписи для физических лиц.

11 Приложение №11. Форма заявления на подтверждение подлинности электронной подписи в электронном документе для юридических лиц и индивидуальных предпринимателей.

12. Приложение №12. Форма заявления на подтверждение подлинности электронной подписи в электронном документе для физических лиц.

13. Приложение №13. Форма копии сертификата ключа проверки электронной подписи на бумажном носителе для юридических лиц и индивидуальных предпринимателей.

14. Приложение №14. Форма копии сертификата ключа проверки электронной подписи на бумажном носителе для физических лиц.

15. Приложение №15. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Приложение № 1
к Регламенту Удостоверяющего центра

Заявление о присоединении к Регламенту
Удостоверяющего центра КГАУ «Информационно-технологический центр»

_____
(наименование организации, включая организационно-правовую форму, ОГРН, ИНН)

в лице_____,
(наименование должности)

_____,
(фамилия, имя, отчество)

действующего на основании_____

_____

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра КГАУ «Информационно-технологический центр», условия которого определены КГАУ «Информационно-технологический центр» и опубликованы на сайте Удостоверяющего центра по адресу http://itc.kamgov.ru/files/uc/accred_reglament.pdf.

С Регламентом Удостоверяющего центра КГАУ «Информационно-технологический центр» и приложениями к нему, ознакомлен (-а) и обязуюсь соблюдать все положения указанного документа.

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

«_____» _____20__года

М.П.

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра КГАУ «Информационно-технологический центр» зарегистрировано в реестре Удостоверяющего центра.
Регистрационный № 12-УЦ-10-02-_____ от «_____» _____ 20___ г

Уполномоченное лицо Удостоверяющего центра КГАУ «Информационно-технологический центр» _____ /_____/
(подпись) (Ф.И.О.)

Печать Удостоверяющего центра

Приложение № 2
к Регламенту Удостоверяющего центра

Заявление о присоединении к Регламенту

Удостоверяющего центра КГАУ «Информационно-технологический центр Камчатского края» *

Я,

_____

(фамилия, имя, отчество)

_____

(серия и номер паспорта

_____

кем и когда выдан),

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра КГАУ «Информационно-технологический», условия которого определены КГАУ «Информационно-технологический центр» и опубликованы на сайте Удостоверяющего центра по адресу http://itc.kamgov.ru/files/uc/accred_reglament.pdf.

С Регламентом Удостоверяющего центра КГАУ «Информационно-технологический центр» и приложениями к нему, ознакомлен (-а) и обязуюсь соблюдать все положения указанного документа.

.

_____ /_____/

(подпись) (Ф.И.О.)

«____» _____ 20__года

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра КГАУ «Информационно-технологический центр Камчатского края» зарегистрировано в реестре Удостоверяющего центра

Регистрационный № 12-УЦ-10-02-_____ от «_____» _____ 20___ г.

Уполномоченное лицо
Удостоверяющего центра КГАУ
«Информационно-технологический центр
Камчатского края»

_____ /_____ /

(подпись) (Ф.И.О.)

Печать Удостоверяющего центра

---

* Заявление о присоединении к Регламенту подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

Приложение № 3
к Регламенту Удостоверяющего центра

Заявление зарегистрировано в УЦ под № 12-УЦ-10-04_____
«_____»_____20__ г.

Заявление
на создание сертификата ключа проверки электронной подписи*

(полное наименование юридического лица согласно Выписке из ЕГРЮЛ _____)
в лице (должность, фамилия, имя, отчество_____),
действующего на основании__ _____
просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи на ключевой носитель для уполномоченного представителя: (фамилия, имя , отчество уполномоченного представителя)_____

В сертификат ключа проверки электронной подписи прошу занести следующие данные:

CommonName (CN)	Сокращенное наименование юридического лица согласно Выписке из ЕГРЮЛ	
INN	Индивидуальный номер налогоплательщика юридического лица	
OGRN/OGRNIP	Основной государственный регистрационный номер юридического лица	
Organization (O)	Сокращенное наименование юридического лица согласно Выписке из ЕГРЮЛ	
Locality (L)	Наименование населённого пункта	Юрид. адрес местонахождения организации
Street Address (STREET)	Улица, номер дома, корпуса, строения, помещения	
State (S)	Наименование субъекта РФ	
Country(C)	RU	
SurName(SN)	Фамилия уполномоченного представителя	
GivenName (G)	Имя и отчество уполномоченного представителя	
Title(T)	Должность уполномоченного представителя	
OrganizationUnit (OU)	Наименование подразделения юридического лица	
SNILS	Страховой номер индивидуального лицевого счёта уполномоченного представителя	
E-Mail (E)	Адрес электронной почты уполномоченного представителя	
Средство электронной подписи	КриптоПро CSP (версия 4.0)	
Дополнительные объектные идентификаторы		
OID		

Настоящим Я,_____
(паспорт гражданина РФ серия _____ № _____ выдан _____)
соглашаюсь на обработку и использование моих персональных данных, указанных в заявительных документах в течении всего срока деятельности Удостоверяющего центра КГАУ «Информационно-технологический центр», также признаю, что персональные данные, заносимые в сертификат ключа проверки электронных подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным; С Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи ознакомлен (-а).

Прошу создать ключ электронной подписи **экспортируемым** (да / нет) _____
(собственноручно)

Контактный телефон Уполномоченного представителя _____

Уполномоченный представитель, данные о котором вносятся в квалифицированный сертификат _____/_____/
(подпись) (Фамилия И.О.)

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

М.П. «_____» _____ 20___г.

* В форму заявления на создание сертификата ключа проверки электронной подписи возможно внесение дополнительных сведений, информации, в случае если сертификат ключа проверки электронной подписи выпускается для использования в информационной системе, имеющей собственные требования к форме такого заявления.

Приложение № 4
к Регламенту Удостоверяющего центра
Заявление зарегистрировано в УЦ под № 12-УЦ-10-04_____
«_____»_____20__ г.

Заявление
на создание сертификата ключа проверки электронной подписи

(полное наименование юридического лица согласно Выписке из ЕГРЮЛ_____)
в лице_(должность, фамилия, имя, отчество_____),
действующего на основании_____
просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи без указания в качестве владельца сертификата ключа проверки электронной подписи физического лица, действующего от имени нашей организации, в сертификате ключа проверки электронной подписи (в том числе в сертификате), используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами.

В сертификат ключа проверки электронной подписи прошу занести следующие данные:

CommonName (CN)	Сокращенное наименование юридического лица согласно Выписке из ЕГРЮЛ	
INN	Индивидуальный номер налогоплательщика юридического лица	
OGRN/OGRNIP	Основной государственный регистрационный номер юридического лица	
Organization (O)	Сокращенное наименование юридического лица согласно Выписке из ЕГРЮЛ	
Locality (L)	Наименование населённого пункта	Юрид. адрес местонахождения организации
Street Address (STREET)	Улица, номер дома, корпуса, строения, помещения	
State (S)	Наименование субъекта РФ	
Country(C)	RU	
E-Mail (E)	Адрес электронной почты уполномоченного представителя	
Средство электронной подписи	КриптоПро CSP (версия 4.0)	

Прошу создать ключ электронной подписи **экспортируемым** (да / нет) __
(собственноручно)

С Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи ознакомлен (-а).

Контактный телефон _____

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

М.П. «_____» _____ 20___г.

Приложение № 5
к Регламенту Удостоверяющего центра
Заявление зарегистрировано в УЦ под № 12-УЦ-10-04_____
«_____»_____20__ г.

Заявление
на создание сертификата ключа проверки электронной подписи

Я, (фамилия, имя, отчество _____)
Паспорт гражданина РФ (серия и номер паспорта, кем и когда выдан_____)
прошу сформировать для ключи электронной подписи и создать сертификат ключа проверки электронной подписи на ключевой носитель.

В сертификат ключа проверки электронной подписи прошу занести следующие данные:

CommonName (CN)	Фамилия, имя и отчество	
INN	Индивидуальный номер налогоплательщика физического лица	
Locality (L)	Наименование населённого пункта	По данным прописки
State (S)	Наименование субъекта РФ	
Country(C)	RU	
SurName(SN)	Фамилия	
GivenName (G)	Имя и отчество	
SNILS	Страховой номер индивидуального лицевого счёта	
E-Mail (E)	Адрес электронной почты	
Средство электронной подписи	КриптоПро CSP (версия 4.0)	
Дополнительные объектные идентификаторы		
OID		

Настоящим Я,_____
даю свое согласие на обработку и использование моих персональных данных, указанных в заявительных документах в течении всего срока деятельности Удостоверяющего центра КГАУ «Информационно-технологический центр», также признаю, что персональные данные, заносимые в сертификат ключа проверки электронных подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным; С Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи ознакомлен (-а).

Контактный телефон _____

_____/_____/
(подпись) (Фамилия И.О.)

«_____» _____ 20___г.

Приложение № 6
к Регламенту Удостоверяющего центра

Доверенность[1]

г. _____ «_____» _____20___ г.

_____
_____
(полное наименование юридического лица согласно Выписке из ЕГРЮЛ)
в лице
_____,
(должность, фамилия, имя, отчество)
действующего на основании _____,
уполномочивает_____
(фамилия, имя, отчество)
Паспорт гражданина РФ_____
(серия и номер паспорта, кем и когда выдан)
действовать от имени_____
(полное наименование юридического лица согласно Выписке из ЕГРЮЛ)

при использовании электронной подписи и осуществлять действия в рамках Регламента Удостоверяющего центра КГАУ «Информационно-технологический центр Камчатского края»

Настоящая доверенность действительна по « ___ » _____20__ г. без права передоверия[2].

Подпись уполномоченного представителя _____ / _____/
подтверждаю. (подпись) (Фамилия И.О)

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

М.П. «_____» _____ 20___г.

[1] Форма доверенности может отличаться от приведенной, если сертификат ключа проверки электронной подписи выпущен для использования в информационной системе, имеющей собственные требования к форме такой доверенности.

[2] Срок доверенности не должен быть меньше срока действия ключа электронной подписи.

Приложение № 7
к Регламенту Удостоверяющего центра

Доверенность

на получение ключевого(-ых) документа(-ов), сертификата(-ов) ключа(-ей) проверки электронной подписи за Владельца(-ев) сертификата в Удостоверяющем центре КГАУ «Информационно-технологический центр»

г. _____ «_____» _____20___ г.

_____
(полное наименование юридического лица согласно Выписке из ЕГРЮЛ)
в лице
_____,
(должность, фамилия, имя, отчество)
действующего на основании _____,
уполномочивает_____
_____
(фамилия, имя, отчество)
Паспорт гражданина РФ_____
(серия и номер паспорта, кем и когда выдан)

Предоставить в Удостоверяющий центр КГАУ «Информационно-технологический центр» необходимые документы, определенные Регламентом Удостоверяющего центра КГАУ «Информационно-технологический центр и получить ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные в Удостоверяющем центре КГАУ «Информационно-технологический центр» за Владельца сертификата

_____
(фамилия, имя, отчество Владельца сертификата)

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

Настоящая доверенность действительна по « ___ » _____ 201__ г. без права передоверия.

Подпись уполномоченного представителя _____/ _____/
подтверждаю. (подпись) (Фамилия И.О)

Подпись Владельца сертификата _____/ _____/
(подпись) (Фамилия И.О)

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

М.П. «_____» _____ 20___г.

Приложение № 8
к Регламенту Удостоверяющего центра

Доверенность*

на получение ключевого(-ых) документа(-ов), сертификата(-ов) ключа(-ей) проверки электронной подписи за Владельца(-ев) сертификата в Удостоверяющем центре КГАУ «Информационно-технологический центр»

г. _____ «_____» _____20___ г.

Я,___
(фамилия, имя, отчество)
Паспорт гражданина РФ_____,
(серия и номер, кем и когда выдан)
уполномочивает_____
(фамилия, имя, отчество)
Паспорт гражданина РФ_____
(серия и номер паспорта, кем и когда выдан)

Предоставить в Удостоверяющий центр КГАУ «Информационно-технологический центр» необходимые документы, определенные Регламентом Удостоверяющего центра КГАУ «Информационно-технологический центр и получить ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные в Удостоверяющем центре КГАУ «Информационно-технологический центр» на моё имя.

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

Настоящая доверенность действительна по « ___ » _____ 201__ г. без права передоверия.

Подпись уполномоченного представителя подтверждаю. _____ / _____/
(подпись) (Фамилия И.О)

_____ / _____/
(подпись) (Фамилия И.О)

«_____» _____ 20___года.

* Данная доверенность должна быть заверена нотариально

Приложение № 9
к Регламенту Удостоверяющего центра

Заявление на аннулирование сертификата ключа проверки электронной подписи

_____
(полное наименование юридического лица согласно Выписке из ЕГРЮЛ)
в лице_____,
(должность, фамилия, имя, отчество)
действующего на основании _____,
в связи с _____,
(причина отзыва сертификата)
просит аннулировать сертификат ключа проверки электронной подписи своего уполномоченного представителя _____
(фамилия, имя, отчество)
содержащий следующие данные:

SerialNumber	Серийный номер сертификата ключа проверки подписи
CommonName (CN)	Фамилия Имя Отчество уполномоченного представителя
INN	ИНН юридического лица/индивидуального предпринимателя
OGRN/OGRNIP	ОГРН для юридического лица, ОГРНИП для индивидуального предпринимателя

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

М.П. «_____» _____ 20___г.

(заполняется сотрудником Удостоверяющего центра)

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

Уполномоченный сотрудник
Удостоверяющего центра КГАУ
/
«Информационно-технологический
центр Камчатского края»

_____ /_____
(подпись) (Ф.И.О.)

Печать Удостоверяющего центра

Приложение № 10
к Регламенту Удостоверяющего центра

Заявление на аннулирование сертификата ключа проверки электронной подписи

Я, _____
(фамилия, имя, отчество)
Паспорт гражданина РФ_____,
(серия и номер, кем и когда выдан)
в связи с _____
(причина отзыва сертификата)

прошу аннулировать сертификат ключа проверки электронной подписи, выданный на мое имя и содержащий следующие данные:

SerialNumber	Серийный номер сертификата ключа проверки подписи
CommonName (CN)	Фамилия, Имя, Отчество
SNILS	СНИЛС физического лица
INN	ИНН физического лица

_____ / _____/
(подпись) (Фамилия И.О)

«___»_____201__года.

(заполняется сотрудником Удостоверяющего центра)

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

Уполномоченный сотрудник
Удостоверяющего центра КГАУ
/
«Информационно-технологический
центр Камчатского края»

_____ /_____
(подпись) (Ф.И.О.)

Печать Удостоверяющего центра

Приложение № 11
к Регламенту Удостоверяющего центра

Заявление на подтверждение подлинности электронной подписи в электронном документе

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

в лице _____,
(должность, фамилия, имя, отчество)

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 USB-носителе.
2. Файл, содержащий подписанные электронной подписью данные и электронную подпись, либо файл CMS, содержащий исходные данные и файл, содержащий значение электронную подпись формата CMS, на прилагаемом к заявлению USB-носителе.
3. Время, подписания электронной подписью электронного документа*:
   «_____:_____» «_____/_____/_____»
   час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого требуется проверить подлинность электронной подписи:
«_____:_____» «_____/_____/_____»
час минута день месяц год

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

М.П. «_____» _____ 20___г.

* Время и дата должны быть указаны с учетом часового пояса г. Петропавловск-Камчатский (по Камчатскому времени). Если время и дата не указаны, то проверка подлинности электронной подписи устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 12
к Регламенту Удостоверяющего центра

Заявление на проверку подтверждение электронной подписи в электронном документе

Я,

_____
(фамилия, имя, отчество)

Паспорт гражданина РФ_____,
(серия и номер, кем и когда выдан)

прошу подтвердить 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 USB-носителе.
2. Файл, содержащий подписанные электронной подписью данные и электронную подпись, либо файл CMS, содержащий исходные данные и файл, содержащий значение электронную подпись формата CMS, на прилагаемом к заявлению USB-носителе.
3. Время, подписания электронной подписью электронного документа*:
   «_____:_____» «_____/_____/_____»
   час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого требуется проверить подлинность электронной подписи:
«_____:_____» «_____/_____/_____»
час минута день месяц год

_____/_____/
(подпись) (Фамилия И.О.)

М.П. «_____» _____ 20___г.

* Время и дата должны быть указаны с учетом часового пояса г. Петропавловск-Камчатский (по Камчатскому времени). Если время и дата не указаны, то проверка подлинности электронной подписи устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 13
к Регламенту Удостоверяющего центра

Удостоверяющий центр КГАУ «Информационно-технологический центр Камчатского края»
Сертификат ключа проверки электронной подписи

Версия: 3
Серийный номер: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Издатель сертификата: CN=КГАУ "Информационно-технологический центр", O=КГАУ "Информационно-технологический центр", STREET=ул. Арсеньева, д. 23, L=г. Петропавловск-Камчатский, S=41 Камчатский край, C=RU, ИНН=004101147350, ОГРН=1114101005600
Владелец сертификата: СНИЛС=XXXXXXXXXXX, ОГРН=XXXXXXXXXXXXX, ОГРНИП=XXXXXXXXXXXXXXX, ИНН = 00XXXXXXXXXX, E = XXX@XXXX.XX, C = RU, S = регион, L = населенный пункт, O = краткое наименование организации, OU = Подразделение, CN = краткое наименование организации, STREET = ул. Улица, д. XX, T = Должность, G=Имя Отчество, SN=Фамилия.
Срок действия:
Действителен с: ДД ММ ГГГГ г. ЧЧ:ММ:СС UTC
Действителен по: ДД ММ ГГГГ г. ЧЧ:ММ:СС UTC
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)
Параметры: XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Значение: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
Расширения сертификата X.509
Расширение: 2.5.29.15 (Использование ключа (критичное))
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
Расширение: 2.5.29.14 (Идентификатор ключа субъекта)
Значение: XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Расширение: 2.5.29.37 (Улучшенный ключ)
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4), ……
Расширение: 1.3.6.1.5.5.7.1.1 (Доступ к информации о центрах сертификации)
Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1), дополнительное имя=URL=http://ocsp.kamgov.ru/ocsp_g2012/ocsp.srf, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://itc.kamgov.ru/files/uc/itckk2019.cer, [3]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://ca.gosuslugi41.ru/files/uc/itckk2019.cer
Расширение: 2.5.29.32 (Политики сертификата)
Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2
Расширение: 1.2.643.100.112 (Средства электронной подписи и УЦ издателя)
Значение: Средство электронной подписи: "КриптоПро CSP" версия 4.0 R4 (исполнение 2-Base) (заключение: Сертификат соответствия № СФ/124-3611 от 10.01.2019), средство удостоверяющего центра: "Программно-аппаратный комплекс "Удостоверяющий центр "КриптоПро УЦ" версии 2.0" (вариант исполения 5) (заключение: Сертификат соответствия № СФ/128-3592 от 17.10.2018)
Расширение: 1.2.643.100.111 (Средство электронной подписи владельца)
Значение: Средство электронной подписи: "КриптоПро CSP"
Расширение: 2.5.29.31 (Точки распространения списков отзыва (CRL))
Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://itc.kamgov.ru/files/uc/itckk2019.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ocsp.kamgov.ru/ocsp/itckk2019.crl, [3]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ca.gosuslugi41.ru/files/uc/itckk2019.crl
Расширение: 1.2.643.2.2.49.2 (Ограниченная лицензия КРИПТО-ПРО)
Значение: Ограниченная лицензия на КриптоПро CSP для использования с закрытым ключом данного сертификата в рамках системы "Проектов Правительства Камчатского края и иных услуг в электронной форме", полный текст доступен по адресу https://itc.kamgov.ru/esignature/ucabout/license

Расширение: 2.5.29.35 (Идентификатор ключа центра сертификатов)

Значение: Идентификатор ключа=684d6dc61a7b35578f4994354f4be4788c40335b, Поставщик сертификата: Адрес каталога:CN=Минкомсвязь России, ИНН=007710474375, ОГРН=1047702026701, O=Минкомсвязь России, STREET="улица Тверская, дом 7", L=г. Москва, S=77 Москва, C=RU, E=dit@minsvyaz.ru, Серийный номер сертификата=7408f2710000000002db

Расширение: 2.5.29.16 (Период использования ключа электронной подписи)

Действителен с ДД ММ ГГГГ г. ЧЧ:ММ:СС UTC по ДД ММ ГГГГ г. ЧЧ:ММ:СС UTC

Подпись Удостоверяющего центра:

Алгоритм подписи: ГОСТ Р 34.11-2012/34.10-2012 256 бит (1.2.643.7.1.1.3.2)

Значение: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Адрес удостоверяющего центра:

683902, Камчатский край, .г. Петропавловск-Камчатский, ул. Арсеньева, д.23

Подпись изготовителя сертификата _____/_____

М. П.

Подпись владельца сертификата _____/_____

"___" _____ 20__ г

Приложение № 14
к Регламенту Удостоверяющего центра

Удостоверяющий центр КГАУ «Информационно-технологический центр Камчатского края»
Сертификат ключа проверки электронной подписи

Версия: 3
Серийный номер: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Издатель сертификата: CN=КГАУ "Информационно-технологический центр", O=КГАУ "Информационно-технологический центр", STREET=ул. Арсеньева, д. 23, L=г. Петропавловск-Камчатский, S=41 Камчатский край, C=RU, ИНН=004101147350, ОГРН=1114101005600
Владелец сертификата: СНИЛС=XXXXXXXXXXX, ИНН = XXXXXXXXXXX, E = XXX@XXXX.XX, C = RU, S = регион, L = населенный пункт, CN = Фамилия Имя Отчество, G=Имя Отчество, SN=Фамилия.
Срок действия:
Действителен с: ДД ММ ГГГГ г. ЧЧ:ММ:СС UTC
Действителен по: ДД ММ ГГГГ г. ЧЧ:ММ:СС UTC
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)
Параметры: XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Значение: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
Расширения сертификата X.509
Расширение: 2.5.29.15 (Использование ключа (критичное))
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
Расширение: 2.5.29.14 (Идентификатор ключа субъекта)
Значение: XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Расширение: 2.5.29.37 (Улучшенный ключ)
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4), ……
Расширение: 1.3.6.1.5.5.7.1.1 (Доступ к информации о центрах сертификации)
Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1), дополнительное имя=URL=http://ocsp.kamgov.ru/ocsp_g2012/ocsp.srf, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://itc.kamgov.ru/files/uc/itckk2019.cer, [3]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://ca.gosuslugi41.ru/files/uc/itckk2019.cer
Расширение: 2.5.29.32 (Политики сертификата)
Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2
Расширение: 1.2.643.100.112 (Средства электронной подписи и УЦ издателя)
Значение: Средство электронной подписи: "КриптоПро CSP" версия 4.0 R4 (исполнение 2-Base) (заключение: Сертификат соответствия № СФ/124-3611 от 10.01.2019), средство удостоверяющего центра: "Программно-аппаратный комплекс "Удостоверяющий центр "КриптоПро УЦ" версии 2.0" (вариант исполения 5) (заключение: Сертификат соответствия № СФ/128-3592 от 17.10.2018)
Расширение: 1.2.643.100.111 (Средство электронной подписи владельца)
Значение: Средство электронной подписи: "КриптоПро CSP"
Расширение: 2.5.29.31 (Точки распространения списков отзыва (CRL))
Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://itc.kamgov.ru/files/uc/itckk2019.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ocsp.kamgov.ru/ocsp/itckk2019.crl, [3]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ca.gosuslugi41.ru/files/uc/itckk2019.crl
Расширение: 1.2.643.2.2.49.2 (Ограниченная лицензия КРИПТО-ПРО)
Значение: Ограниченная лицензия на КриптоПро CSP для использования с закрытым ключом данного сертификата в рамках системы "Проектов Правительства Камчатского края и иных услуг в электронной форме", полный текст доступен по адресу https://itc.kamgov.ru/esignature/ucabout/license

Расширение: 2.5.29.35 (Идентификатор ключа центра сертификатов)
Значение: Идентификатор ключа=684d6dc61a7b35578f4994354f4be4788c40335b, Поставщик сертификата: Адрес каталога:CN=Минкомсвязь России, ИНН=007710474375, ОГРН=1047702026701, O=Минкомсвязь России, STREET="улица Тверская, дом 7", L=г. Москва, S=77 Москва, C=RU, E=dit@minsvyaz.ru, Серийный номер сертификата=7408f2710000000002db
Подпись Удостоверяющего центра:
Алгоритм подписи: ГОСТ Р 34.11-2012/34.10-2012 256 бит (1.2.643.7.1.1.3.2)
Значение: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Адрес удостоверяющего центра:
683902, Камчатский край, .г. Петропавловск-Камчатский, ул. Арсеньева, д.23

Подпись изготовителя сертификата _____/_____

М. П.

Подпись владельца сертификата _____/_____
"___" _____ 20__ г

Приложение № 15
к Регламенту Удостоверяющего центра

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Обеспечьте конфиденциальность ключей электронной подписи.
2. Для предотвращения внештатных ситуаций при использовании ключевой информации **ограничьте доступ к компьютеру**, который используется для работы с ключевой информацией и подписания документов электронной подписью. Не доверяйте Ваш компьютер для обслуживания посторонним лицам, исключите бесконтрольный доступ в помещения, в которых размещаются средства электронной подписи.
3. **Не передавайте никому личный ключевой носитель и не сообщайте PIN-код к нему** кому бы то ни было. Доступ к ключевому носителю должен быть только у владельца электронной подписи.
4. **Не оставляйте личный ключевой носитель и/или PIN-код доступа к нему без присмотра.**
5. Обеспечьте безопасное хранение ключей электронной подписи на ключевом носителе в сейфе или запираемом ящике стола.
6. **Подсоединяйте ключевой носитель к компьютеру только для подписания электронных документов**, и в обязательном порядке извлекайте его из компьютера сразу после окончания работы. Блокируйте компьютер и извлекайте ключевые носители при уходе с рабочего места.
7. **Не извлекайте ключевой носитель во время его работы**, т.к. это может привести к потере данных на нем. Извлечение ключевого носителя должно производиться через «Безопасное извлечение Запоминающего устройства».
8. **Старайтесь не наносить повреждений своему ключевому носителю**, не ронять и не ударять, а при извлечении из порта компьютера не менять угол наклона и не раскачивать. Механические повреждения могут привести к поломке ключевого носителя.
9. Не допускается снимать несанкционированные копии с ключевых носителей, знакомить или передавать ключевые носители лицам, к ним не допущенным, записывать на ключевой носитель с ключами электронной подписи постороннюю информацию.
10. **Работайте под учетной записью обычного пользователя** (учетная запись должна быть защищена надежным паролем). Не рекомендуется работа с электронной подписью под учетной записью «Администратор». Отключите стандартную учетную запись «Гость».
11. Запретите доступ по сети в вашей организации к каталогам на компьютере, где установлены средства электронной подписи, посторонним лицам.
12. Используйте на компьютере только лицензионное программное обеспечение. Своевременно устанавливайте обновления безопасности операционной системы.

13. **Обеспечьте непрерывную комплексную защиту компьютера от вирусов**, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ лицензионным антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления баз данных, с включенной защитой паролем и сетевой защитой, выставленной на максимальный уровень безопасности. Будьте очень осторожны при получении сообщений файлами-вложениями. Обращайте внимание на расширение файла. Проводите полную еженедельную проверку компьютера на наличие вирусов.
14. Применяйте для формирования электронной подписи только действующий ключ электронной подписи и с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy), если такие ограничения были установлены.
15. В случае утраты личного ключевого носителя и/или PIN-кода доступа к нему для блокировки использования Вашего ключа электронной подписи посторонними лицами **немедленно известите Удостоверяющий центр о нарушении конфиденциальности ключа электронной подписи**. Не применяйте ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
16. Немедленно обратитесь в Удостоверяющий центр с заявлением на аннулирование сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
17. Используйте для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
18. **Запрещается устанавливать режим «Включить кэширование»** в настройках режима работы средства электронной подписи. Кэширование заключается в том, что считанные с ключевого носителя ключи останутся загруженными в памяти службы хранения ключей и будут доступны любому приложению после извлечения ключевого носителя из считывателя и до завершения работы компьютера. Это означает, что в случае хакерской атаки на Ваш компьютер, злоумышленник сможет воспользоваться загруженными ключами для выработки электронной подписи от Вашего имени.
19. Если вам в течение сеанса работы со средствами электронной подписи приходится многократно использовать ключевой носитель, то для ускорения работы используйте настройку средства электронной подписи «Запомнить пароль». **После завершения сеанса работы обязательно удалите запомненные пароли**, для чего используйте возможности средства электронной подписи.
20. В организации соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств электронной подписи, назначены владельцы средств электронной подписи и должностные лица, ответственные за обеспечение

безопасности информации и эксплуатации этих средств; средства электронной подписи и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах.