Утвержден
Приказом Руководителя
Краевого государственного казенного учреждения
«Центр информационных технологий Красноярского края»
№ 120-д от «08» 02 2018 г.

СОГЛАСОВАНО
Руководитель Агентства информатизации и связи Красноярского края

_____ Н.А. Распопин
«28» 02 2018 г.

УТВЕРЖДАЮ
Руководитель Краевого государственного казенного учреждения «Центр информационных технологий Красноярского края»

_____ Е.В. Дружинин
«01» 03 2018 г.

РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ

Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(версия 2.2)

г. Красноярск 2018 г.

СОДЕРЖАНИЕ

1. Сведения об Удостоверяющем центре

Краевой удостоверяющий центр электронного правительства Красноярского края (далее – УЦ) является элементом инфраструктуры «Электронного правительства» Красноярского края (ЭПКК), обеспечивающим на безвозмездной основе создание квалифицированных сертификатов ключей проверки электронной подписи уполномоченных сотрудников органов, входящих в систему органов государственной власти Красноярского края и иных государственных органов Красноярского края, органов местного самоуправления Красноярского края, а также подведомственных учреждений вышеперечисленных органов (далее – органы государственной власти Красноярского края).

УЦ развернут и функционирует на базе программно-аппаратного комплекса «КриптоПро УЦ» версии 2.0 (Сертификат соответствия ФСБ России № СФ/128-2881 от 30.12.2016).

Юридическим лицом, на базе которого действует УЦ, а также которое уполномочено осуществлять управление и обеспечение работы УЦ, является Краевое государственное казённое учреждение «Центр информационных технологий Красноярского края».

Краевое государственное казенное учреждение «Центр информационных технологий Красноярского края» (далее – КГКУ «ЦИТ»), зарегистрировано на территории Российской Федерации в городе Красноярске (Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1102468001316 от 18.01.2010 г.).

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании:

Свидетельства об аккредитации удостоверяющего центра № 812 от 28 ноября 2017 г., выданного Министерством связи и массовых коммуникаций Российской Федерации.

Лицензии Управления ФСБ России по Красноярскому краю рег. № 266 Н от 16 ноября 2016 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Реквизиты КГКУ «ЦИТ»:

Полное наименование: Краевое государственное казённое учреждение «Центр информационных технологий Красноярского края»

Юридический адрес: 660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176

Адрес нахождения Удостоверяющего центра: 660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176

Адрес для корреспонденции: 660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176

Банковские реквизиты (наименование банка, БИК, р/с, к/с):
БИК 040407001
р/с 40201810000000000003
в Отделении Красноярск г. Красноярск
ИНН/КПП: 2466226448/246001001
ОГРН: 1102468001316
Код по ОКВЭД: 62.09, 18.2, 33.13, 41.2, 43.2, 61.1, 61.10.4, 61.10.9, 62.0, 62.02, 63.1, 63.11.1, 74.20, 74.30, 82.92, 95.1
Код по ОКПО: 64089776

Контактная информация:

тел. +7 (391) 263-17-68 – оператор Удостоверяющего центра (ул. Робеспьера, 32);
тел. +7 (391) 263-10-20, 263-10-25 – техническая поддержка КГКУ «ЦИТ»;
тел. +7 (391) 263-10-47, 263-10-38 – администратор Удостоверяющего центра;
e-mail: kuc@krskcit.ru
Адрес УЦ в сети Интернет: http://www.it.krskstate.ru/udostov_centr

2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

Администратор Удостоверяющего центра – сотрудник КГКУ «ЦИТ», наделенный соответствующими полномочиями по настройке, обслуживанию, обеспечению работоспособности и безопасности Удостоверяющего центра.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в соответствии с законодательством Российской Федерации и настоящим Регламентом выдан сертификат ключа проверки электронной подписи.

Инфраструктура – информационно-технологическая и коммуникационная инфраструктура, обеспечивающая информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме. (Федеральный закон от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", Постановление Правительства РФ от 22 декабря 2012 г. № 1382)

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

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

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует (не приостановлен и не аннулирован) на указанный момент времени.

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 Удостоверяющего центра – ключ электронной подписи, использующийся Удостоверяющим центром для создания сертификатов ключей проверки электронной подписи и/или 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.

Компрометация ключа электронной подписи – хищение, утрата действующего ключа электронной подписи или его носителя, передача или сообщение его лицам, не имеющим на то право, другие действия сотрудника, приведшие к его получению лицами, не имеющими на то право. Скомпрометированные ключи электронной подписи выводятся из действия немедленно.

Пользователь Удостоверяющего центра (Пользователь УЦ) – лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец ключа проверки

электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи в информационной системе.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 09:00 по 18:00 (время красноярское) каждого дня недели за исключением выходных и праздничных дней.

Реестр Удостоверяющего центра – набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- список зарегистрированных пользователей Удостоверяющего центра;
- заявления на изготовление сертификатов ключей проверки электронной подписи;
- заявления на прекращение (аннулирование, отзыв) сертификатов ключей проверки электронной подписи;
- заявления на приостановление/возобновление действия сертификатов ключей проверки электронной подписи;
- заявления на подтверждение подлинности электронной подписи в электронном документе;
- сертификаты ключей проверки электронной подписи;
- списки отозванных сертификатов.

Сертификат ключа проверки электронной подписи (СКПЭП) – электронный документ, выданный Удостоверяющим центром 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 и действие его не приостановлено.

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

Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в электронных ответах Службы актуальных статусов сертификатов, содержащих информацию о статусе сертификатов, выданных Удостоверяющим центром.

Сертификат ключа проверки электронной подписи Службы штампов времени Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в штампах времени, сформированных Службой штампов времени Удостоверяющего центра.

Служба актуальных статусов сертификатов – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого подписываются

квалифицированной электронной подписью и предоставляются Пользователям УЦ электронные ответы, содержащие информацию о статусе сертификатов, выданных Удостоверяющим центром.

Служба штампов времени – сервис Удостоверяющего центра (построенный на базе протокола TSP), с использованием которого подписываются квалифицированной электронной подписью и предоставляются Пользователям УЦ штампы времени.

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

Средство криптографической защиты информации (СКЗИ) – программное или аппаратное средство, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

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

Стороны Регламента Удостоверяющего центра – КГКУ «ЦИТ» и органы государственной власти Красноярского края, являющиеся сторонами Соглашения о безвозмездном оказании услуг Удостоверяющего центра.

Удостоверяющий центр – Краевое государственное казенное учреждение «Центр информационных технологий Красноярского края», осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи». Удостоверяющий центр с момента аккредитации уполномоченным федеральным органом исполнительной власти Российской Федерации в сфере использования электронной подписи осуществляет создание и выдачу квалифицированных сертификатов ключей проверки электронной подписи.

Уполномоченное лицо (Оператор) Удостоверяющего центра – сотрудник КГКУ «ЦИТ», наделенный от имени Удостоверяющего центра полномочиями по созданию ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра (выдача, аннулирование, приостановление и возобновление действия), по заверению электронной подписью сертификатов ключей проверки электронной подписи и списков отозванных сертификатов, а также заверению собственноручной подписью копий сертификатов ключей проверки электронной подписи на бумажных носителях.

Штамп времени электронного документа (штамп времени) – электронный документ, подписанный квалифицированной электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

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.

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.

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

Online Certificate Status Protocol (OCSP) – протокол установления статуса сертификата ключа проверки электронной подписи, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».

Time-Stamp Protocol (TSP) – протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)».

3. Общие положения

3.1. Регламент деятельности УЦ по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность аккредитованных удостоверяющих центров.

3.2. Статус Регламента

Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра.

Настоящий Регламент распространяется:

форме электронного документа:

по адресу: URL=http://www.it.krskstate.ru/udostov_centr/reglament.pdf

форме документа на бумажном носителе:

при письменном обращении в Удостоверяющий центр.

3.3. Настоящий Регламент является документом, определяющим условия предоставления и правила пользования услугами УЦ, включая права, обязанности, ответственность Сторон Регламента, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы УЦ.

3.4. Настоящий Регламент согласовывается с Агентством информатизации и связи Красноярского края, утверждается руководителем КГКУ «ЦИТ» и вводится в действие его приказом.

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

3.6. Присоединение к Регламенту

3.6.1. Присоединение к настоящему Регламенту осуществляется путем подписания с КГКУ «ЦИТ» Соглашения о безвозмездном оказании услуг удостоверяющего центра (далее – Соглашение) по форме Приложения №11 к Регламенту.

3.6.2. Соглашение может быть заключено только после получения согласования Агентства информатизации и связи Красноярского края.

3.6.3. Удостоверяющий центр вправе отказать любому лицу в подписании Соглашения, регистрации пользователей УЦ и издании им СКПЭП, при отсутствии согласования со стороны Агентства информатизации и связи Красноярского края.

3.6.4. Факт подписания Соглашения является полным принятием его Стороной условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Соглашения. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения и/или дополнения, вносимые в Регламент, в соответствии с условиями настоящего Регламента.

3.6.5. В случае расторжения Соглашения Удостоверяющий центр принимает меры по аннулированию СКПЭП всех пользователей УЦ, являющихся уполномоченными представителями Стороны данного Соглашения.

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

3.7. Изменение Регламента

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

3.7.2. Внесение изменений (дополнений) в Регламент, а также в приложения к нему, производится путем подготовки и утверждения очередной редакции Регламента, которая согласовывается с Агентством информатизации и связи Красноярского края, утверждается руководителем КГКУ «ЦИТ» и вводится в действие его приказом.

3.7.3. Измененный текст Регламента должен быть опубликован на сайте в сети Интернет по адресу http://www.it.krskstate.ru/udostov_centr/reglament.pdf не позднее 3-х рабочих дней с даты его утверждения.

3.7.4. Все изменения, вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении тридцати календарных дней с даты размещения указанных изменений в Регламенте на сайте УЦ по адресу – http://www.it.krskstate.ru/udostov_centr/reglament.pdf

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

3.8. Термины, применяемые в настоящем Регламенте, понимаются строго в контексте общего смысла Регламента.

3.9. В случае противоречия и/или расхождения названия какого-либо раздела настоящего Регламента со смыслом одного из его пунктов, считается доминирующим смысл и формулировки каждого конкретного пункта.

3.10. В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями Регламента, считается доминирующим смысл и формулировки Регламента.

4. Предоставление информации

4.1. Удостоверяющий центр предоставляет Пользователю УЦ, по его требованию:

- Копию имеющейся действующей лицензии ФСБ России на осуществление деятельности в области шифрования информации;
- Копию действующей редакции Регламента Удостоверяющего центра;

- Копию свидетельства об аккредитации Удостоверяющего центра.

4.2. Удостоверяющий центр вправе запросить у Пользователя УЦ, а Пользователь УЦ обязан представить Удостоверяющему центру документы, подтверждающие следующую информацию:

- документы, подтверждающие наименование организации, полномочным представителем которой является Пользователь УЦ, основной государственный регистрационный номер, идентификационный номер налогоплательщика;
- копию Устава организации (заверенную организацией или нотариально – по усмотрению Удостоверяющего центра);
- копию свидетельства о государственной регистрации юридического лица (заверенную организацией или нотариально – по усмотрению Удостоверяющего центра);
- копии протоколов, решений, приказов, распоряжений либо иных документов о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и/или надлежащим образом оформленные доверенности;
- копию приказа о назначении Пользователя УЦ на должность, которая будет указана в сертификате ключа проверки электронной подписи;
- сведения, необходимые для идентификации Пользователя УЦ: копию, документа, признаваемого в соответствии с законодательством Российской Федерации документом, удостоверяющими личность, содержащую информацию о его реквизитах (серия, номер, дата выдачи и кем выдан), а также о фамилии, имени, отчестве (при наличии) и месте регистрации, а также копию СНИЛС и ИНН;
- копию документа, подтверждающего полномочия Пользователя УЦ для включения дополнительных объектных идентификаторов (в расширение EKU) в его сертификат ключа проверки электронной подписи, дающих Пользователю УЦ право использовать электронную подпись в каких-либо специализированных областях применения.

5. Права и обязанности Удостоверяющего центра и Пользователя УЦ

5.1. Удостоверяющий центр обязан:

5.1.1. Предоставлять услуги по созданию ключей электронной подписи и квалифицированных сертификатов ключей проверки электронных подписей органам государственной власти Красноярского края на безвозмездной основе при условии установления личности получателя сертификата (заявителя) и полномочий лица, выступающего от имени заявителя.

5.1.2. Предоставить Пользователю Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра, а также сертификаты ключа проверки электронной подписи Удостоверяющих центров, стоящих выше по иерархии, в электронной форме.

5.1.3. Использовать в своей деятельности только средства электронной подписи и средства удостоверяющего центра, получившие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

5.1.4. Использовать ключ электронной подписи Удостоверяющего центра только для подписи издаваемых им сертификатов ключей проверки электронной подписи и/или списков отозванных сертификатов.

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

5.1.6. Организовать свою работу по красноярскому времени (UTC +07:00). Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

5.1.7. Обеспечить регистрацию пользователей в Удостоверяющем центре на основании заявлений на создание сертификатов ключей проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.8. Обеспечить уникальность идентификационных данных Пользователей УЦ, заносимых в сертификаты ключей проверки электронной подписи.

5.1.9. Изготовить сертификат ключа проверки электронной подписи Пользователя УЦ по заявлению на создание сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.10. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки электронной подписи.

5.1.11. Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.1.12. Вести реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей (далее – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

5.1.13. Обеспечить сохранение в тайне созданного ключа электронной подписи Пользователя Удостоверяющего центра в случае его создания на территории Удостоверяющего центра.

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

5.1.15. Прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра, если истек установленный срок, на который действие данного сертификата было приостановлено.

5.1.16. Прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра.

5.1.17. Официально уведомить об аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации списка

отозванных сертификатов в течение двенадцати часов с момента аннулирования (отзыва), приостановления и возобновления действия сертификата.

5.1.18. Публиковать актуальные списки отозванных сертификатов с периодичностью – 1 раз в сутки. Адреса размещения списков отозванных сертификатов включать в создаваемые сертификаты ключей проверки электронной подписи в расширение CDP (CRL Distribution Point).

5.1.19. Осуществлять по обращениям Стороны Соглашения проверку электронных подписей.

5.1.20. Устанавливать сроки действия сертификатов ключей проверки электронных подписей, создаваемых Удостоверяющим центром.

5.1.21. Информировать Пользователей УЦ 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.

5.1.22. Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к реестру квалифицированных сертификатов Удостоверяющего центра в любое время в течение срока деятельности Удостоверяющего центра, в том числе к спискам отозванных сертификатов.

5.1.23. В случае принятия решения о прекращении деятельности Удостоверяющего центра:

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

5.2. Организация (Сторона Соглашения), уполномоченным представителем которой является Пользователь УЦ, обязана:

5.2.1. С целью обеспечения гарантированного ознакомления с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу http://www.it.krskstate.ru/udostov_centr/reglament.pdf с целью получения сведений об изменениях и дополнениях, включенных в Регламент.

5.2.2. Требовать от своих уполномоченных представителей (Пользователей Удостоверяющего центра) исполнения следующих обязанностей:

5.2.2.1. Обеспечивать конфиденциальность ключей электронной подписи.

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

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

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

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

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

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

5.2.2.8. Не использовать ключ электронной подписи до предоставления Удостоверяющему центру подписанной копии сертификата ключа проверки электронной подписи, соответствующего данному ключу электронной подписи.

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

5.2.3. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи Пользователя УЦ, а также в случае если уполномоченный сотрудник организации (Пользователь УЦ) более не является таковым по причине его увольнения, смерти, прекращения действия или истечения срока доверенности, трудового договора, а также в случае перевода его на другую работу и т.п.

5.3. Удостоверяющий центр имеет право:

5.3.1. Отказать пользователю в регистрации в Удостоверяющем центре в случае ненадлежащего оформления необходимых заявительных документов.

5.3.2. Отказать в создании сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на создание сертификата ключа проверки электронной подписи и иных необходимых документов, а также при отсутствии согласования Агентства информатизации и связи Красноярского края о возможности создания СКПЭП для уполномоченных сотрудников организации и отсутствии заключенного с КГКУ «ЦИТ» Соглашения.

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

5.3.4. Отказать в прекращении, приостановлении и/или возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего

центра в случае, если истек установленный срок действия сертификата ключа проверки электронной подписи этого Пользователя УЦ.

5.3.5. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра с обязательным уведомлением владельца сертификата ключа проверки электронной подписи, действие которого приостановлено, и указанием обоснованных причин.

5.4. Пользователь Удостоверяющего центра имеет право:

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

5.4.2. Применять списки отозванных сертификатов ключей проверки электронной подписи, созданные Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

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

5.4.4. Получить копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра.

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

5.4.6. Пользоваться сервисами Службы актуальных статусов сертификатов и Службы штампов времени Удостоверяющего центра.

6. Порядок предоставления и пользования услугами Удостоверяющего центра

6.1. Формирование ключей электронной подписи и создание сертификатов ключей проверки электронной подписи (первого[1] сертификата ключа проверки электронной подписи, при плановой и внеплановой смене ключа электронной подписи) Удостоверяющий центр осуществляет только юридическим лицам (их уполномоченным представителям), которые являются стороной Соглашения.

Изготовление сертификата ключа проверки электронной подписи осуществляется на основании заявления на изготовление сертификата ключа проверки электронной подписи при личном прибытии Пользователя УЦ в офис КГКУ «ЦИТ» по адресу нахождения Удостоверяющего центра либо путем направления в УЦ уполномоченного представителя Пользователя УЦ по доверенности.

Форма заявления на изготовление сертификата ключа проверки электронной подписи приведена в Приложении №1-а (для сотрудника организации) или Приложении №1-б (для информационной системы организации) к настоящему Регламенту. При оформлении заявления на изготовление сертификата ключа проверки электронной подписи заявитель в том числе указывает ключевую фразу, которая предназначена для аутентификации Пользователя Удостоверяющего центра (применяемую Пользователем

[1] В контексте настоящего регламента «первым» сертификатом ключа проверки электронной подписи Пользователя УЦ считается сертификат, впервые создаваемый Удостоверяющим центром для нового Пользователя УЦ.

УЦ при обращении в Удостоверяющий центр по телефону) при выполнении регламентных процедур, возникающих при нарушении конфиденциальности (компрометации) ключа электронной подписи Пользователя УЦ.

При создании сертификата ключа проверки электронной подписи 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 №2 к настоящему Регламенту и быть действительной на момент создания сертификата ключа проверки электронной подписи.

Регламентом УЦ определен следующий состав заявительных документов для изготовления сертификата ключа проверки электронной подписи:

1. Заявление на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ (по форме Приложения №1-а к Регламенту).
2. Заверенная надлежащим образом копия доверенности или иной документ (в простой письменной форме на бланке организации-заявителя), подтверждающий полномочия подписанта Заявления на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ, в случае если данное Заявление подписано исполняющим обязанности руководителя организации-заявителя или иным лицом по доверенности.
3. Доверенность Пользователя УЦ (по форме Приложения №2 к Регламенту) в случае, если Пользователь УЦ не является руководителем организации-заявителя.
4. Доверенность на получение ключа электронной подписи и сертификата ключа проверки электронной подписи за Пользователя УЦ (по форме Приложения №3-а к Регламенту) в случае, если в Удостоверяющий центр направляется уполномоченный представитель Пользователя УЦ.
5. Копия приказа о назначении на должность уполномоченного представителя организации-заявителя (Пользователя УЦ), заверенная руководителем организации-заявителя датой, не превышающей одного месяца до момента подачи заявительных документов в Удостоверяющий центр.
6. Основной документ (оригинал), удостоверяющий личность Пользователя УЦ, или его надлежащим образом заверенная копия (разворот 2-й и 3-й страниц, а также страница с последним адресом регистрации по месту жительства).
7. Оригинал или заверенная надлежащим образом копия страхового свидетельства государственного пенсионного страхования (СНИЛС) Пользователя УЦ.
8. Оригинал или заверенная надлежащим образом копия свидетельства о постановке на учет в налоговом органе (ИНН) Пользователя УЦ (физического лица).
9. Оригинал или заверенная надлежащим образом копия свидетельства о государственной регистрации (ОГРН) организации-заявителя.
10. Основной документ (оригинал), удостоверяющий личность уполномоченного представителя Пользователя УЦ, действующего по доверенности от имени Пользователя УЦ.
11. Согласия на обработку персональных данных (по форме Приложения №13 к Регламенту) от Пользователя УЦ, а также от его уполномоченного представителя по доверенности.

12. Чистый USB-flash диск для записи ключа электронной подписи, сертификата ключа проверки электронной подписи, цепочки сертификатов Удостоверяющего центра и вышестоящих удостоверяющих центров и иных документов, включая настоящий Регламент и иные инструкции и методические материалы, связанные с настройкой и использованием электронной подписи.

При подаче заявления на изготовление сертификата ключа проверки электронной подписи юридического лица, предназначенного для автоматического создания электронных подписей (для информационной системы) применяется форма Приложения №1-б настоящего Регламента. При этом комплект заявительных документов подается в Удостоверяющий центр в следующем составе:

1. Заявление на изготовление сертификата ключа проверки электронной подписи информационной системы организации (по форме Приложения №1-б к Регламенту).
2. Заверенная надлежащим образом копия доверенности или иной документ (по форме организации-заявителя), подтверждающий полномочия подписанта Заявления на изготовление сертификата ключа проверки электронной подписи, в случае если данное Заявление подписано исполняющим обязанности руководителя организации-заявителя или иным лицом по доверенности.
3. Доверенность на получение ключа электронной подписи и сертификата ключа проверки электронной подписи (по форме Приложения №3-б к Регламенту), выданную уполномоченному представителю организации-заявителя.
4. Оригинал или заверенная надлежащим образом копия свидетельства о государственной регистрации (ОГРН) организации-заявителя.
5. Основной документ (оригинал), удостоверяющий личность уполномоченного представителя организации-заявителя, действующего по доверенности (по форме Приложения №3-б к Регламенту).
6. Согласие на обработку персональных данных (по форме Приложения №13 к Регламенту) от уполномоченного представителя организации-заявителя по доверенности.
7. Чистый USB-flash диск для записи ключа электронной подписи, сертификата ключа проверки электронной подписи, цепочки сертификатов Удостоверяющего центра и вышестоящих удостоверяющих центров и иных документов.

Предоставление в Удостоверяющий центр заявительных документов, описанных в настоящем пункте Регламента, осуществляется только полным комплектом (как при регистрации нового Пользователя УЦ и изготовлении его первого сертификата ключа проверки электронной подписи, так и при плановой или внеплановой смене сертификата).

При предоставлении организацией-заявителем в Удостоверяющий центр не полного или не должным образом оформленного пакета документов, Удостоверяющий центр имеет право не принимать их к исполнению.

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

- физическим лицом (действующим от имени юридического лица на основании Устава или доверенности по форме Приложения №2 к Регламенту), которое указывается в сертификате наряду с наименованием юридического лица;

- другим физическим лицом (уполномоченным представителем пользователя Удостоверяющего центра) на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложений №3-а или №3-б к настоящему Регламенту.

Оператор Удостоверяющего центра при получении комплекта заявительных документов от организации-заявителя устанавливает личность его уполномоченного представителя, на чьё имя требуется создать сертификат ключа проверки электронной подписи (Пользователя УЦ), личность лица, предоставившего документы в Удостоверяющий центр по доверенности от имени Пользователя УЦ, комплектность и правильность оформления заявительных документов, а также запрашивает и получает через инфраструктуру из государственных информационных ресурсов выписку из единого государственного реестра юридических лиц (ЕГРЮЛ) в отношении организации-заявителя, с которой сравнивает информацию, предоставленную в комплекте заявительных документов, в том числе сведения о лице, имеющем право без доверенности действовать от имени юридического лица.

Если заявителем в Удостоверяющий центр предоставляются оригиналы документов Пользователя УЦ, то Оператор УЦ снимает с них копии, подписывает их у Пользователя УЦ (или его уполномоченного представителя), а также самостоятельно заверяет их путем нанесения на каждую копию отметки «БЫЛ ПРЕДЪЯВЛЕН ОРИГИНАЛ», ставит свою роспись и печать Удостоверяющего центра.

После успешной проверки комплекта заявительных документов Оператор Удостоверяющего центра на их основе осуществляет регистрацию Пользователя УЦ в реестре Удостоверяющего центра (в случае создания первого СКПЭП), выполняет действия по формированию ключа электронной подписи на предоставленный заявителем USB-flash диск и созданию сертификата ключа проверки электронной подписи, который также записывается на предоставленный USB-flash диск.

Оператор Удостоверяющего центра передает сформированный ключевой носитель представителю организации-заявителя и распечатывает в двух экземплярах на бумажном носителе информацию, содержащуюся в созданном сертификате ключа проверки электронной подписи, в виде копии сертификата, оформленной по форме Приложения №9 к настоящему Регламенту.

Два экземпляра копии сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра на бумажном носителе визируются Оператором Удостоверяющего центра, заверяются печатью Удостоверяющего центра и передаются Пользователю Удостоверяющего центра.

Пользователь УЦ (либо его уполномоченный представитель по доверенности) подписывает собственноручной подписью два экземпляра копии сертификата ключа проверки электронной подписи на бумажном носителе и один экземпляр возвращает Оператору Удостоверяющего центра. Если за Пользователя УЦ копии сертификата подписывает его полномочный представитель, то на каждом экземпляре копии сертификата ключа проверки электронной подписи обязательно указывается номер и дата доверенности, на основании которой действует данный уполномоченный представитель Пользователя УЦ.

По окончании процедуры создания сертификата ключа проверки электронной подписи Пользователю Удостоверяющего центра выдаются:

- ключевой носитель (ранее предоставленный заявителем для генерации ключа электронной подписи), содержащий контейнер ключа электронной подписи (*Пользователю УЦ рекомендуется сделать резервную копию ключа электронной подписи на любой другой отчуждаемый носитель, поддерживаемый программным обеспечением криптопровайдера, и хранить его в недоступном для посторонних лиц месте*);

- пароль доступа к ключевому контейнеру, который был использован для формирования ключа электронной подписи Оператором Удостоверяющего центра (*после получения от Удостоверяющего центра ключевого носителя Пользователю УЦ рекомендуется самостоятельно осуществить смену пароля доступа к ключевому контейнеру штатными средствами программного обеспечения криптопровайдера*);
- файл сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра, соответствующий его ключу электронной подписи;
- файл сертификата ключа проверки электронной подписи Удостоверяющего центра, а также файлы сертификатов ключей проверки электронной подписи удостоверяющих центров, находящихся выше по иерархии;
- копия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (один экземпляр) на бумажном носителе.

Если ключи электронной подписи и сертификаты ключей проверки электронной подписи юридического лица будут использоваться для автоматического создания электронных подписей, то допускается не указывать в качестве владельца сертификата ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, при этом в сертификат ключа проверки электронной подписи значение СНИЛС не включается.

6.2. Прекращение действия (аннулирование, отзыв) сертификата ключа проверки электронной подписи

Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра в следующих случаях:

- при расторжении Соглашения, Стороной которого является организация, уполномоченным представителем которой является Пользователь УЦ.
- по истечении срока, на который действие сертификата было приостановлено;
- по письменному заявлению владельца сертификата ключа проверки электронной подписи (Приложение №4-а) или организации, уполномоченным представителем которой он является или являлся (Приложение №4-б);
- на основании вступившего в законную силу решения суда, которым в частности установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи Пользователя УЦ.

В случае прекращения действия сертификата ключа проверки электронной подписи, истечения срока, на который действие сертификата было приостановлено, по заявлению владельца сертификата, по решению суда, вступившего в законную силу, Удостоверяющий центр официально уведомляет владельца сертификата и всех Пользователей Удостоверяющего центра о прекращении действия сертификата ключа проверки электронной подписи.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование в течение двенадцати часов последнего списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было прекращено. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной

подписи в расширение «CRL Distribution Point» сертификата ключа проверки электронной подписи.

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

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

6.2.1. Прекращение действия сертификата ключа проверки электронной подписи по заявлению в бумажной форме.

Подача заявления в Удостоверяющий центр на прекращение действия сертификата ключа проверки электронной подписи может быть осуществлена Пользователем УЦ (владельцем сертификата отзываемого ключа проверки электронной подписи) по форме Приложения №4-а к Регламенту или организацией, уполномоченным представителем которой он является или являлся, путем оформления заявления по форме Приложения №4-б к Регламенту и направления его в Удостоверяющий центр посредством почтовой или курьерской связи на адрес Удостоверяющего центра (660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176).

В заявлении в обязательном порядке указывается одна из следующих причин отзыва сертификата:

- Компрометация ключа электронной подписи[1]
- Изменение принадлежности[2]
- Замена сертификата[3]
- Прекращение работы[4].

Заявления на прекращение действия (аннулирование, отзыв) сертификата ключа проверки электронной подписи без указания причины отзыва Удостоверяющим центром не принимаются.

После получения Удостоверяющим центром заявления на прекращение действия сертификата ключа проверки электронной подписи Оператор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на прекращение действия сертификата должна быть осуществлена в срок, не превышающий двенадцати часов с момента, когда указанное заявление было принято Удостоверяющим центром.

---

[1] В случае если Пользователь УЦ (владелец СКПЭП) допустил утерю носителя ключа ЭП, нарушение конфиденциальности пароля доступа к ключевому контейнеру либо имеется достаточно оснований для подозрения в таком нарушении, например, при вирусном заражении компьютера Пользователя УЦ.

[2] Например, в случае изменения фамилии, должности или других реквизитов Пользователя УЦ (владельца СКПЭП). Либо если сертификат, выданный на информационную систему, более не принадлежит этой организации или этой информационной системе, а также в случае изменения реквизитов организации.

[3] В случае если для Пользователя УЦ создается новый сертификат ключа проверки электронной подписи при плановой смене до истечения срока предыдущего сертификата.

[4] В случае увольнения или иного прекращения работы Пользователя УЦ в качестве сотрудника организации, у которой заключено соглашение с Удостоверяющим центром. При этом подписать заявление на отзыв сертификата ключа проверки электронной подписи может как сам владелец сертификата, так и руководитель организации, сотрудником которой являлся владелец аннулируемого сертификата.

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

При принятии положительного решения Оператор Удостоверяющего центра аннулирует действие сертификата ключа проверки электронной подписи и осуществляет внеочередной выпуск CRL.

6.2.2. Прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в связи с расторжением Соглашения.

В случае расторжения Соглашения по инициативе любой из Сторон, Удостоверяющим центром, с момента подписания Сторонами дополнительного соглашения о расторжении Соглашения, осуществляются действия по аннулированию (отзыву) сертификатов ключей проверки электронных подписей всех Пользователей УЦ, являвшихся уполномоченными представителями организации, у которой с Удостоверяющим центром было заключено данное Соглашение.

6.3. Приостановление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

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

- по заявлению владельца сертификата ключа проверки электронной подписи (по форме Приложения №5-а к Регламенту) или организации, уполномоченным представителем которой он является (по форме Приложения №5-б к Регламенту);
- по заявлению владельца сертификата ключа проверки электронной подписи в устной форме в случае компрометации или подозрения в компрометации ключа электронной подписи;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

Действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра приостанавливается на срок до определенной даты включительно. Минимальный срок приостановления действия сертификата ключа проверки электронной подписи составляет 10 календарных дней, максимальный срок – до даты окончания действия сертификата ключа проверки электронной подписи.

По истечению срока приостановления действия сертификата ключа проверки электронной подписи данный сертификат будет автоматически аннулирован Удостоверяющим центром либо действие данного сертификата будет автоматически возобновлено Удостоверяющим центром в зависимости от требований, изложенных в заявлении на приостановление действия сертификата.

Официальным уведомлением о факте приостановления действия сертификата ключа проверки электронной подписи является опубликование в течение двенадцати часов последнего списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

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

6.3.1. Приостановление действия сертификата ключа проверки электронной подписи по заявлению в бумажной форме.

Подача заявления в Удостоверяющий центр на приостановление действия сертификата ключа проверки электронной подписи может быть осуществлена посредством почтовой или курьерской связи по форме Приложений №5-а или №5-б к Регламенту на адрес Удостоверяющего центра (660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176).

После получения Удостоверяющим центром заявления на приостановление действия сертификата ключа проверки электронной подписи Оператор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена в срок, не превышающий двенадцати часов с момента, когда указанное заявление было принято Удостоверяющим центром.

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

При принятии положительного решения Оператор Удостоверяющего центра приостанавливает действие сертификата ключа проверки электронной подписи и осуществляет внеочередной выпуск CRL.

6.3.2. Приостановление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по его заявлению в устной форме.

Приостановление действия сертификата ключа проверки электронной подписи по заявке в устной форме осуществляется исключительно при нарушении конфиденциальности ключа электронной подписи или подозрении в нарушении конфиденциальности ключа электронной подписи Пользователя Удостоверяющего центра.

Заявление подается в Удостоверяющий центр по телефону Оператора Удостоверяющего центра, указанному в разделе 1 настоящего Регламента.

При обращении в Удостоверяющий центр с заявлением в устной форме о приостановлении действия сертификата ключа проверки электронной подписи Пользователь Удостоверяющего центра должен сообщить Оператору Удостоверяющего центра следующую информацию:

- идентификационные данные Пользователя УЦ, содержащиеся в сертификате ключа проверки электронной подписи, действие которого необходимо приостановить;
- ключевую фразу Пользователя УЦ (ключевая фраза определяется в процессе регистрации Пользователя Удостоверяющего центра);
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;

Заявление в устной форме принимается Удостоверяющим центром только при положительной аутентификации Пользователя Удостоверяющего центра (в том числе совпадения ключевой фразы, произнесенной заявителем, с информацией из реестра зарегистрированных Пользователей Удостоверяющего центра).

После принятия заявления Оператор Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа проверки электронной подписи. Принятие решения о приостановлении действия сертификата должно быть осуществлено немедленно с момента поступления данного заявления.

В случае отказа в приостановлении действия сертификата ключа проверки электронной подписи Пользователь Удостоверяющего центра уведомляется об этом с указанием причины отклонения заявки.

При принятии положительного решения Оператор Удостоверяющего центра приостанавливает действие сертификата ключа проверки электронной подписи на срок до окончания срока действия ключа электронной подписи, соответствующего данному сертификату.

Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата ключа проверки электронной подписи Пользователь Удостоверяющего центра должен предоставить в Удостоверяющий центр заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи в бумажной форме (в том случае, если факт компрометации ключа электронной подписи подтвердился), либо заявление на возобновление действия сертификата ключа проверки электронной подписи (в том случае, если решение о компрометации ключа электронной подписи было ошибочно принято Пользователем УЦ).

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

Удостоверяющий центр вправе приостановить действие сертификата ключа проверки электронной подписи в случаях получения информации о нарушении конфиденциальности или подозрения в нарушении конфиденциальности соответствующего ключа электронной подписи в том случае, если владельцу сертификата ключа проверки электронной подписи не было известно о возможном факте нарушения конфиденциальности его ключей, на основании ставшей известной Удостоверяющему центру информации о том, что Пользователь УЦ более не является уполномоченным представителем организации, которым он являлся в момент изготовления его сертификата ключа проверки электронной подписи, а также в случаях неисполнения владельцем сертификата ключа проверки электронной подписи обязательств по настоящему Регламенту либо на основании правомерного мотивированного письменного запроса или предписания уполномоченных государственных органов.

После приостановления действия сертификата ключа проверки электронной подписи Оператор Удостоверяющего центра сообщает владельцу сертификата ключа проверки электронной подписи о наступлении события, повлекшего приостановление действие сертификата, и уведомляет его о том, что действие сертификата приостановлено. Уведомление осуществляется по электронной почте на адрес, указанный при регистрации Пользователя УЦ.

6.4. Возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра только по письменному заявлению организации (Стороны Соглашения) и только в том случае, если действие соответствующего сертификата ключа проверки электронной подписи было приостановлено.

Подача заявления в Удостоверяющий центр на возобновление действия сертификата ключа проверки электронной подписи осуществляется руководителем организации (Стороны Соглашения) посредством почтовой или курьерской связи по форме Приложения №6 к Регламенту на адрес Удостоверяющего центра (660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176).

Возобновление действия сертификата ключа проверки электронной подписи возможно только в течение срока, на который действие сертификата ключа проверки электронной подписи было приостановлено.

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

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

При принятии положительного решения Оператор Удостоверяющего центра возобновляет действие сертификата ключа проверки электронной подписи и осуществляет внеочередной выпуск CRL.

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

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

6.5. Получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром.

Получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром, осуществляется на основании заявления Стороны, заключившей Соглашение с Удостоверяющим центром. Данное заявление оформляется по форме Приложения №7 к Регламенту и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи на адрес Удостоверяющего центра (660021, г. Красноярск, ул. Робеспьера, д. 32, помещение № 176).

Заявление должно содержать следующую информацию:

- дату подачи заявления;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа проверки электронной подписи;
- идентификационные данные пользователя Удостоверяющего центра, статус сертификата ключа проверки электронной подписи которого требуется установить;
- серийный номер сертификата ключа проверки электронной подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа проверки электронной подписи, которая предоставляется заявителю.

Предоставление заявителю справки о статусе сертификата ключа проверки электронной подписи должно быть осуществлено не позднее 10 (Десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

6.6. Подтверждение подлинности электронной подписи в электронном документе

По желанию Стороны, заключившей Соглашение с Удостоверяющим центром, Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению подлинности электронной подписи в электронном документе.

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

Для проверки подлинности электронной подписи в электронных документах Сторона, присоединившаяся к Регламенту, подает заявление в Удостоверяющий центр по форме Приложения №8 к Регламенту.

Заявление должно содержать следующую информацию:

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

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

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

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

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

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки электронной подписи электронного документа;
- данные, представленные комиссии для проведения проверки.
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

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

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

6.7. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени.

6.7.1. Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Выполнены условия признания квалифицированной электронной подписи в OCSP-ответе;
- Квалифицированная электронная подпись в OCSP-ответе сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы актуальных статусов сертификатов, а именно: сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов в расширении Enhanced Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.9 – «Подпись ответа службы OCSP».

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – http://uc.krskcit.ru:8081/ocsp/ocsp.srf. Указанный адрес заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центром сертификатов ключей проверки электронной подписи.

6.7.2. Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному электронной подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

- Выполнены условия признания квалифицированной электронной подписи в штампе времени;
- Квалифицированная электронная подпись в штампе времени сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы штампов времени, а именно: сертификат ключа

проверки электронной подписи Службы штампов времени в расширении Enhanced Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.8 – «Установка штампа времени»

Адрес обращения к Службе штампов времени Удостоверяющего центра – http://uc.krskcit.ru:8081/tsp/tsp.srf.

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

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

Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи может быть занесена следующая информация:

- в поле Subject (идентифицирует владельца сертификата):
  - Поле E (Email) – адрес электронной почты;
  - Поле T (Title) – должность уполномоченного представителя юридического лица, данные которого занесены в сертификат наряду с наименованием юридического лица;
- 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 +7:00;
  Действителен по (notAfter): дд.мм.гггг чч:мм:сс UTC +7:00;
- расширение «Enhanced Key Usage» (Улучшенный ключ, Расширенное использование ключа) – набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с сертификатом ключа проверки электронной подписи (если такие ограничения установлены);
- расширение «CRL Distribution Point» (Точка распространения списка отозванных сертификатов) – набор адресов точек распространения списков отозванных сертификатов;
- расширение «Authority Information Access» (Доступ к информации о центре) – адрес обращения к Службе актуальных статусов сертификатов, адрес размещения сертификата Удостоверяющего центра;
- иные поля и расширения по усмотрению Удостоверяющего центра.

7.2. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

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

		Конкретный перчень полей устанавливается Удостоверяющим центром
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC +7:00
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC +7:00
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reason Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, которым подписан СОС
CA Version	Версия сертификата издателя	Версия сертификата Центра сертификации
CRL Number	Номер СОС	Порядковый номер СОС
CRL Next Publish	Следующая публикация СОС	дд.мм.гггг чч:мм:сс UTC +7:00

7.3. Расширения «Key Usage», «Enhanced Key Usage», «Application Policy», «Certificate Policies» сертификата ключа проверки электронной подписи содержат объектные идентификаторы (OID), определяющие отношения, при которых электронный документ, подписанный электронной подписью, будет иметь юридическое силу.

7.4. Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре и определяющих отношения, при которых электронный документ, подписанный электронной подписью, будет иметь юридическую силу, приведен в Приложении № 10 настоящего Регламента.

7.5. Сроки действия ключевых документов

7.5.1. Сроки действия ключевых документов Удостоверяющего центра

Срок действия ключа электронной подписи Удостоверяющего центра составляет 3 года (максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной

подписи, с использованием которого данный ключ электронной подписи был сформирован).

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

Срок действия сертификата ключа проверки электронной подписи Удостоверяющего центра определяется регламентом вышестоящего по иерархии удостоверяющего центра и составляет 10 лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

Срок действия ключа электронной подписи Службы актуальных статусов сертификатов составляет 15 месяцев.

Начало периода действия ключа электронной подписи Службы актуальных статусов сертификатов исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов.

Срок действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов не превышает 15 месяцев. Время начала периода действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

Срок действия ключа электронной подписи Службы штампов времени составляет 15 месяцев.

Начало периода действия ключа электронной подписи Службы штампов времени исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы штампов времени.

Срок действия сертификата ключа проверки электронной подписи Службы штампов времени не превышает 15 месяцев. Время начала периода действия сертификата ключа проверки электронной подписи Службы штампов времени и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

7.5.2. Сроки действия ключевых документов Пользователей Удостоверяющего центра

Срок действия ключа электронной подписи Пользователя Удостоверяющего центра составляет 15 месяцев. Начало периода действия ключа электронной подписи Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра составляет 15 месяцев. Время начала периода действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

8. Дополнительные положения

8.1. Плановая смена ключей Удостоверяющего центра

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

Процедура плановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

- Удостоверяющий центр формирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр проводит процедуру получения нового сертификата ключа проверки электронной подписи Удостоверяющего центра в Уполномоченном федеральном органе в области использования электронной подписи.

Уведомление пользователей о проведении смены ключей уполномоченного лица Удостоверяющего центра осуществляется посредством размещения соответствующей информации на сайте Удостоверяющего центра в сети Интернет по адресу http://www.it.krskstate.ru/udostov_centr.

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

8.2. Компрометация (нарушение конфиденциальности) ключевых документов Удостоверяющего центра, внеплановая смена ключей Удостоверяющего центра

В случае компрометации ключа электронной подписи Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра аннулируется (прекращает всё действие), Пользователи Удостоверяющего центра уведомляются об указанном факте путем публикации информации о компрометации на сайте Удостоверяющего центра в сети Интернет по адресу http://www.it.krskstate.ru/udostov_centr.. Все сертификаты (в том числе пользовательские), подписанные с использованием скомпрометированного ключа электронной подписи Удостоверяющего центра, считаются аннулированными.

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

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

8.3. Компрометация ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи.

В случае компрометации или угрозы компрометации ключа электронной подписи Пользователь обращается в Удостоверяющий центр по телефону и приостанавливает действие своего сертификата в соответствии с положениями п.6.3.2 настоящего Регламента.

8.4. Конфиденциальность информации

8.4.1. Типы конфиденциальной информации

8.4.1.1. Ключ электронной подписи, а также пароль доступа к контейнеру ключа электронной подписи, являются конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключей

электронных подписей Пользователей Удостоверяющего центра и паролей доступа к ним.

8.4.1.2. Персональная и корпоративная информация о Пользователях Удостоверяющего центра, не подлежащая непосредственной рассылке или опубликованию в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

8.4.2. Типы информации, не являющейся конфиденциальной

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

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

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

8.4.2.4. Персональные данные, включаемые в сертификаты ключей проверки электронных подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным. Реестр сертификатов ключей проверки электронной подписи подлежит публикации в общем доступе в соответствии с требованиями закона №63-ФЗ от 06.04.2011 «Об электронной подписи».

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

8.4.3. Исключительные полномочия Удостоверяющего центра

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

8.5. Хранение сертификатов ключей проверки электронной подписи в Удостоверяющем центре

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

8.6. Прекращение оказания услуг Удостоверяющим центром

В случае расторжения Соглашения, прекращается действие всех сертификатов ключей проверки электронной подписи Пользователей УЦ, имеющих отношение к Стороне, заключившей данное Соглашение с Удостоверяющим центром.

8.7. Непреодолимая сила (форс-мажор)

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

8.7.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования 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.

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

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

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

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

Приложение №1-а
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ***)

Заявление на создание квалифицированного сертификата
ключа проверки электронной подписи

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

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

действующего на основании _____

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

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

_____
(фамилия, имя, отчество Пользователя УЦ)

Паспорт: серия _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____
ИНН Пользователя УЦ (физического лица) _____

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

Название поля сертификата	**Значение поля сертификата**
CommonName (CN)	*Наименование организации в строгом соответствии с ЕГРЮЛ – **максимум 64 символа***
Organization (O)	*Наименование организации в строгом соответствии с ЕГРЮЛ*
OrganizationUnit (OU)	*Наименование подразделения Пользователя УЦ*
SurName (SN)	*Фамилия Пользователя УЦ*
GivenName (GN)	*Имя и Отчество Пользователя УЦ*
Title (T)	*Должность Пользователя УЦ*
E-Mail (E)	*Адрес электронной почты Пользователя УЦ*
Locality (L)	*Наименование населенного пункта организации*
State (S)	**24 Красноярский край**
Country (C)	**RU**
INN	*ИНН организации (**12 цифр – с двумя лидирующими нулями**)*
OGRN	*ОГРН организации (**13 цифр**)*
SNILS	*СНИЛС Пользователя УЦ (**11 цифр**)*

и следующие расширения сертификата:

OIDы расширения «Enhanced Key Usage» («Улучшенный ключ»):

OID	Назначение
1.3.6.1.5.5.7.3.2	Client Authentication (Проверка подлинности клиента)
1.3.6.1.5.5.7.3.4	Secure Email (Защищенная электронная почта)
Дополнительные OIDы расширения «Улучшенный ключ»[1]	

OIDы расширения «Certificate Policy» («Политика сертификата»):

OID	Значение[2]
1.2.643.100.113.1	Класс средства ЭП КС1
1.2.643.100.113.2	Класс средства ЭП КС2

OID расширения «Subject sign tool» («Средство ЭП владельца»):

OID	Значение[3]
1.2.643.100.111	*Наименование и версия средства электронной подписи*

В реквизиты Пользователя в реестре УЦ прошу включить следующую дополнительную информацию:

Адрес электронной почты для получения уведомлений от УЦ	*Адрес электронной почты для получения уведомлений от УЦ*
Ключевая фраза[4]	

Настоящим _____
(Фамилия, Имя, Отчество Пользователя УЦ)

Паспорт: серия _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____
соглашается с обработкой своих персональных данных Удостоверяющим центром (КГКУ «Центр информационных технологий Красноярского края») и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра _____
(Подпись)

«____» _____ 20____ г.

Должность руководителя организации _____ _____
(Подпись) (Фамилия И.О.)

дата подписания
Печать организации

[1] В данную таблицу можно также включить дополнительные объектные идентификаторы, которые требуется включить в сертификат ключа проверки электронной подписи Пользователя УЦ. В графу «OID» необходимо включать значение объектного идентификатора, а в графу «Назначение» – его описание в соответствии с Приложением №10 настоящего Регламента. Необходимые дополнительные OIDы заявитель выбирает самостоятельно, исходя из потребностей информационной системы, в которой будет применяться ключ электронной подписи, а также с учётом принадлежности организации-заявителя к соответствующему типу органа государственной власти.

[2] OID 1.2.643.100.113.1 (Класс средства ЭП КС1) является обязательным,
OID 1.2.643.100.113.2 (Класс средства ЭП КС2) необходимо включать только в случае необходимости, вызванной требованиями информационной системы. При добавлении данного OIDa в сертификат пользователя УЦ к компьютеру, на котором будет применяться ключ электронной подписи предъявляются дополнительные требования, в том числе: на рабочем месте пользователя необходимо использовать аппаратный датчик случайных чисел, а также применять СКЗИ «КриптоПро CSP», имеющее сертификат соответствия ФСБ России требованиям по классу КС2.

[3] Необходимо указать средство электронной подписи, применяемое на компьютере Пользователя УЦ, например: СКЗИ «КриптоПро CSP» (версия 4.0) или иной версии, реально используемой на рабочем месте Пользователя УЦ.

[4] Ключевая фраза – кодовое слово и набор слов, которые будут использоваться Пользователем УЦ при устном обращении в Удостоверяющий центр для приостановления сертификата ключа проверки электронной подписи в случае компрометации ключа электронной подписи Пользователя УЦ.

Приложение №1-б
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на изготовление сертификата ключа проверки электронной подписи для информационной системы***)

Заявление на создание квалифицированного сертификата
ключа проверки электронной подписи

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

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

действующего на основании _____

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

Сертификат ключа проверки электронный подписи предназначен для:

_____
(наименование информационной системы)

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

Название поля сертификата	**Значение поля сертификата**
CommonName (CN)	*Наименование информационной системы или иное отображаемое имя по требованиям информационной системы – **максимум 64 символа***
Organization (O)	*Наименование организации в строгом соответствии с ЕГРЮЛ*
OrganizationUnit (OU)	*Наименование подразделения ответственного за информационную систему*
SurName (SN)	*Фамилия ответственного за информационную систему*
GivenName (GN)	*Имя и Отчество ответственного за информационную систему*
Title (T)	*Должность ответственного за информационную систему*
E-Mail (E)	*Адрес электронной почты ответственного за информационную систему*
Locality (L)	*Наименование населенного пункта организации*
State (S)	**24 Красноярский край**
Country (C)	**RU**
INN	*ИНН организации (**12 цифр – с двумя лидирующими нулями**)*
OGRN	*ОГРН организации (**13 цифр**)*

и следующие расширения сертификата:

OIDы расширения «Enhanced Key Usage» («Улучшенный ключ»):

OID	**Назначение**
1.3.6.1.5.5.7.3.2	Client Authentication (Проверка подлинности клиента)
1.3.6.1.5.5.7.3.4	Secure Email (Защищенная электронная почта)
Дополнительные OIDы расширения «Улучшенный ключ»[1]	

OIDы расширения «Certificate Policy» («Политика сертификата»):

OID	**Значение**[2]
1.2.643.100.113.1	Класс средства ЭП КС1
1.2.643.100.113.2	Класс средства ЭП КС2

OID расширения «Subject sign tool» («Средство ЭП владельца»):

OID	**Значение**[3]
1.2.643.100.111	*Наименование и версия средства электронной подписи*

В реквизиты Пользователя в реестре УЦ прошу включить следующую дополнительную информацию:

Адрес электронной почты для получения уведомлений от УЦ	*Адрес электронной почты для получения уведомлений от УЦ*
Ключевая фраза[4]	

Должность руководителя организации _____ (Подпись) _____ (Фамилия И.О.)

дата подписания
Печать организации

[1] В данную таблицу можно также включить дополнительные объектные идентификаторы, которые требуется включить в сертификат ключа проверки электронной подписи Пользователя УЦ. В графу «OID» необходимо включать значение объектного идентификатора, а в графу «Назначение» – его описание в соответствии с Приложением №10 настоящего Регламента. Необходимые дополнительные OIDы заявитель выбирает самостоятельно, исходя из потребностей информационной системы, в которой будет применяться ключ электронной подписи.

[2] OID 1.2.643.100.113.1 (Класс средства ЭП КС1) является обязательным,

OID 1.2.643.100.113.2 (Класс средства ЭП КС2) необходимо включать только в случае необходимости, вызванной требованиями информационной системы. При добавлении данного OIDa в сертификат пользователя УЦ к компьютеру, на котором будет применяться ключ электронной подписи предъявляются дополнительные требования, в том числе: на рабочем месте пользователя необходимо использовать аппаратный датчик случайных чисел, а также применять СКЗИ «КриптоПро CSP», имеющее сертификат соответствия ФСБ России требованиям по классу КС2.

[3] Необходимо указать средство электронной подписи, применяемое на сервере информационной системы, например: СКЗИ «КриптоПро CSP» (версия 4.0) или иной версии, реально используемой на рабочем месте Пользователя УЦ.

[4] Ключевая фраза – кодовое слово и набор слов, которые будут использоваться организацией при устном обращении в Удостоверяющий центр для приостановления сертификата ключа проверки электронной подписи в случае компрометации ключа электронной подписи информационной системы.

Приложение №2
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма доверенности Пользователя Удостоверяющего центра***)

Доверенность №_____

г. _____ «_____» _____20___ г.

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

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

действующего на основании _____

уполномочивает _____
(Фамилия, Имя, Отчество Пользователя УЦ)

Паспорт: серия _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____
выступать от имени нашей организации в роли Пользователя Краевого Удостоверяющего центра электронного правительства Красноярского края (ЭПКК) и осуществлять действия в рамках Регламента Удостоверяющего центра ЭПКК по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, установленные для Пользователя Удостоверяющего центра ЭПКК.

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

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

Должность руководителя организации _____ (Подпись) _____ (Фамилия И.О.)

дата подписания
Печать организации

Приложение №3-а
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма доверенности на получение ключа электронной подписи и сертификата ключа проверки электронной подписи за Пользователя УЦ***)

Доверенность №_____

г. _____ «_____» _____20___ г.

Настоящей доверенностью я, _____
(Фамилия, Имя, Отчество Пользователя УЦ)

Паспорт: серия _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____

Уполномочиваю своего представителя _____
(Фамилия, Имя, Отчество представителя Пользователя УЦ)

Паспорт: серия _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____
совершать следующие действия:

1. Предоставить в Краевой Удостоверяющий центр электронного правительства Красноярского края (ЭПКК) необходимые документы, определенные Регламентом деятельности УЦ, для изготовления ключа электронной подписи и сертификата ключа проверки электронной подписи на моё имя.
2. Получить в Краевом Удостоверяющем центре ЭПКК ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные на моё имя, а также сертификат ключа проверки электронной подписи Удостоверяющего центра ЭПКК.
3. Расписываться в соответствующих документах, в том числе на копиях сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе, выданного на моё имя.

Настоящая доверенность выдана по «___»_____ 20__ г. без права передоверия.

Собственноручную подпись представителя удостоверяю. _____ (Подпись) _____ (Фамилия И.О.)

Пользователь Удостоверяющего центра ЭПКК _____ (Подпись) _____ (Фамилия И.О.)

«____» _____ 20____ г.

Должность руководителя организации _____ (Подпись) _____ (Фамилия И.О.)

дата подписания
Печать организации

Приложение №3-б
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма доверенности на получение ключа электронной подписи и сертификата ключа проверки электронной подписи для информационной системы***)

Доверенность №_____

г. _____ «_____» _____20___ г.

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

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

действующего на основании _____

уполномочивает _____
(Фамилия, Имя, Отчество Пользователя УЦ)

Паспорт: серия _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____
совершать следующие действия:

1. Предоставить в Краевой Удостоверяющий центр электронного правительства Красноярского края (ЭПКК) необходимые документы, определенные Регламентом деятельности УЦ, для изготовления ключа электронной подписи и сертификата ключа проверки электронной подписи.
2. Получить в Краевом Удостоверяющем центре ЭПКК ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные для

_____
(наименование информационной системы)

3. Расписываться в соответствующих документах, в том числе на копиях сертификата ключа проверки электронной подписи на бумажном носителе, выданного для

_____
(наименование информационной системы)

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

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

Должность руководителя организации _____ (Подпись) _____ (Фамилия И.О.)

дата подписания
Печать организации

Приложение №4-а
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на прекращение действия (аннулирование, отзыв) сертификата ключа проверки электронной подписи от имени Пользователя УЦ***)

Заявление на прекращение действия (аннулирование, отзыв)
сертификата ключа проверки электронной подписи

Я, _____
(Фамилия, Имя, Отчество Пользователя УЦ)

документ, удостоверяющий личность: _____
Серия: _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____
прошу аннулировать (отозвать) сертификат ключа проверки электронной подписи, выданный на моё имя:

SerialNumber (SN)[1]	
Причина отзыва[2]	

Пользователь УЦ _____ _____
(Подпись) (Фамилия И.О.)

«____» _____ 20____ г.

[1] Серийный номер сертификата ключа проверки электронной подписи, который требуется отозвать
[2] В соответствии с пунктом 6.2.1. Регламента УЦ

Приложение №4-б
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на прекращение действия (аннулирование, отзыв) сертификата ключа проверки электронной подписи от имени организации***)

Заявление на прекращение действия (аннулирование, отзыв)
сертификата ключа проверки электронной подписи

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

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

действующего на основании _____

Просит аннулировать (отозвать) сертификат ключа проверки электронной подписи:

_____
(фамилия, имя, отчество Пользователя УЦ или наименование информационной системы)

SerialNumber (SN)[1]	
Причина отзыва[2]	

Должность руководителя организации _____ _____
(Подпись) (Фамилия И.О.)

дата подписания
Печать организации

[1] Серийный номер сертификата ключа проверки электронной подписи, который троебуется отозвать
[2] В соответствии с пунктом 6.2.1. Регламента УЦ

Приложение №5-а
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на приостановление действия сертификата ключа проверки электронной подписи от имени Пользователя УЦ***)

Заявление на приостановление действия
сертификата ключа проверки электронной подписи

Я, _____
(Фамилия, Имя, Отчество Пользователя УЦ)

документ, удостоверяющий личность: _____
Серия: _____ № _____
Выдан: _____
Код подразделения: _____
Дата выдачи: _____

прошу приостановить действие сертификата ключа проверки электронной подписи, выданного на моё имя:

SerialNumber (SN)[1]	

Срок приостановления действия сертификата[2]: до _____ включительно
(дата)

По окончанию срока приостановления вышеуказанного сертификата прошу:
☐ возобновить его действие ☐ отозвать (аннулировать) его

Пользователь УЦ _____ _____
(Подпись) (Фамилия И.О.)

«____» _____ 20____ г.

[1] Серийный номер сертификата ключа проверки электронной подписи, действие которого надо приостановить

[2] Приостановление действия СКПЭП может быть осуществлено на срок не менее 10 (десяти) календарных дней

Приложение №5-б
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на приостановление действия сертификата ключа проверки электронной подписи от имени организации***)

Заявление на приостановление действия
сертификата ключа проверки электронной подписи

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

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

действующего на основании _____

Просит приостановить действие сертификата ключа проверки электронной подписи, выданного на имя:

_____
(фамилия, имя, отчество Пользователя УЦ или наименование информационной системы)

SerialNumber (SN)[1]	

Срок приостановления действия сертификата[2]: до _____ включительно
(дата)

По окончанию срока приостановления вышеуказанного сертификата прошу:
☐ возобновить его действие ☐ отозвать (аннулировать) его

Должность руководителя организации _____ _____
(Подпись) (Фамилия И.О.)

дата подписания
Печать организации

[1] Серийный номер сертификата ключа проверки электронной подписи, действие которого надо приостановить

[2] Приостановление действия СКПЭП может быть осуществлено на срок не менее 10 (десяти) календарных дней

Приложение №6
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на возобновление действия сертификата ключа проверки электронной подписи***)

Заявление на возобновление действия сертификата
ключа проверки электронной подписи

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

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

действующего на основании _____

Просит возобновить действие сертификата ключа проверки электронной подписи, выданного на имя:

_____
(фамилия, имя, отчество Пользователя УЦ или наименование информационной системы)

SerialNumber (SN)[1]	

Должность руководителя организации _____ _____
(Подпись) (Фамилия И.О.)

дата подписания
Печать организации

[1] Серийный номер сертификата ключа проверки электронной подписи, действие которого требуется возобновить

Приложение №7
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи***)

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Краевым Удостоверяющим центром электронного правительства Красноярского края (ЭПКК)

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

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

действующего на основании _____

Просит предоставить информацию о статусе следующего сертификата ключа проверки электронной подписи:

SerialNumber (SN)[1]	
Время[2] (период времени) на момент наступления которого требуется установить статус сертификата:	с __:__ «___» _____ 20__ г. по __:__ «___» _____ 20__ г.

Должность руководителя организации _____ _____
(Подпись) (Фамилия И.О.)

дата подписания
Печать организации

[1] Серийный номер сертификата ключа проверки электронной подписи, статус которого требуется проверить

[2] Время и дата должны быть указаны с учетом часового пояса г. Красноярска (по красноярскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №8
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма заявления на подтверждение подлинности электронной подписи в электронном документе***)

Заявление на подтверждение подлинности электронной подписи
в электронном документе

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

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

действующего на основании _____

Просит 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 носителе – рег. № _____;

2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № _____;

3. Время[1] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»
час минута день месяц год

Должность руководителя организации _____ _____
(Подпись) (Фамилия И.О.)

дата подписания
Печать организации

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

Приложение №9
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма копии сертификата ключа проверки электронной подписи на бумажном носителе***)

Удостоверяющий Центр электронного правительства Красноярского края
Сертификат ключа проверки электронной подписи

Сведения о сертификате:

Версия: 3
Серийный номер: 05EEEE052BD93CA5A7E711B5583757C9B1
Издатель сертификата: CN=CA KGKU CIT, OU=отдел информационной безопасности, O=КГКУ "ЦИТ", L=Красноярск, S=24 Красноярский край, C=RU, E=info@krskcit.ru, OID.1.2.643.3.131.1.1=002466226448, OID.1.2.643.100.1=1102468001316, STREET=ул. Робеспьера, д. 32, пом. 176
Владелец сертификата: CN=КГКУ "ЦИТ", OU=Бухгалтерия, O=КГКУ "ЦИТ", L=Красноярск, S=24 Красноярский край, C=RU, STREET=пр. Мира, д.91, SNILS=08512326981, OGRN=1102468001316, INN=002466226448, SN=Иванов, G=Петр Иванович, E=ivanov@krskcit.ru

Срок действия:
Действителен с: 24.06.2017 15:08:26
Действителен по: 24.09.2018 15:18:26

Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 0440 56CB 1225 1A3E 3413 9474 A8C9 A551 0679 BE43 A970 0D65 E07F 6734 1194 7C5D F60A 7B3A 208B EA1F AF10 C622 4BC5 4B69 30C7 41DB 9DDC 3439 132E 57B3 82DC A77F A18C

Расширения сертификата X.509
Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Шифрование ключей, Согласование ключей (a8)
Расширение: Идентификатор ключа субъекта
Идентификатор: 2.5.29.14
Значение: 8e 48 0d 40 63 66 1d fd 67 23 63 2e 28 4a 53 4b 19 a4 3b 12
Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=d6 9b ad e6 ca f6 80 ac b7 bc d3 97 43 3f 26 4a 69 fa bb 71, Поставщик сертификата: Адрес каталога:CN=Головной удостоверяющий центр, OID.1.2.643.3.131.1.1=007710474375, OID.1.2.643.100.1=1047702026701, O=Минкомсвязь России, STREET="125375 г. Москва, ул. Тверская, д. 7", L=Москва, S=77 г. Москва, C=RU, E=dit@minsvyaz.ru, Серийный номер сертификата=00 99 5c e0 a0 00 00 00 00 01 24
Расширение: Улучшенный ключ
Идентификатор: 2.5.29.37
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: Политики применения
Идентификатор: 1.3.6.1.4.1.311.21.10
Значение: [1]Политика сертификата приложения:Идентификатор политики=Проверка подлинности клиента, [2]Политика сертификата приложения:Идентификатор политики=Защищенная электронная почта
Расширение: Политики сертификата
Идентификатор: 2.5.29.32
Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1

Расширение: Issuer sign tool
Идентификатор: 1.2.643.100.112
Значение: Средство электронной подписи: ПАКМ "КриптоПро HSM" (версия 1.0) (заключение: Сертификат соответствия № СФ/121-3145 от 17.06.2017), средство удостоверяющего центра: ПАК "Удостоверяющий центр "КриптоПро УЦ" (версия 2.0) (заключение: Сертификат соответствия № СФ/128-2881 от 30.12.2016)
Расширение: Subject sign tool
Идентификатор: 1.2.643.100.111
Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0)
Расширение: Точки распространения списков отзыва (CRL)
Идентификатор: 2.5.29.31
Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://crl.kuc.krskcit.ru/r5.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://uc.krskcit.ru/cdp/r5.crl
Расширение: Доступ к информации о центрах сертификации
Идентификатор: 1.3.6.1.5.5.7.1.1
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://uc.krskcit.ru:8081/ocsp/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://cdp.kuc.krskcit.ru/ca_kgku_cit(5).crt
Расширение: Период использования ключа электронной подписи
Идентификатор: 2.5.29.16
Значение: Действителен с 24 июня 2017 г. 15:08:26 по 24 сентября 2018 г. 15:08:26

Подпись Удостоверяющего центра:

Алгоритм подписи: ГОСТ Р 34.11/34.10-2001 (1.2.643.2.2.3)
Параметры:
Значение: D9AE 3A6A 953E 0642 4211 FD14 3AAB A163 B93C 70C4 5FF8 0780 460B 6641 BA37 A844 9C30 399F 45C1 B92F 6BEC C64D E9F9 7FD6 43D6 4F29 C068 1D44 1AAB C2B3 DDB8 3E12

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

По доверенности №_____ от "___"_____ 20__г.

Подпись уполномоченного лица УЦ: _____/_____

"___" _____ 20__ г.

М. П.

Приложение №10
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи

Список объектных идентификаторов (OID), зарегистрированных в Краевом Удостоверяющем центре электронного правительства Красноярского края и определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение

OID	**Область применения**
Обязательные объектные идентификаторы, включаемые Удостоверяющим центром в сертификаты ключей проверки электронной подписи	
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента
1.3.6.1.5.5.7.3.4	Защищенная электронная почта
Объектные идентификаторы для доступа к СМЭВ	
1.2.643.100.2.1	Доступ к СМЭВ уполномоченного лица органа власти (ЭП-СП)
1.2.643.100.2.2	Доступ к СМЭВ юридического лица (органа власти) (ЭП-ОВ)

Объектные идентификаторы, которые могут быть включены Удостоверяющим центром в СКПЭП Пользователей УЦ для электронного взаимодействия с Росреестром, и соответствующие им субъекты, имеющие право на получение квалифицированного сертификата ключа проверки электронной подписи, содержащего данный OID			
OID	Ограничение использования квалифицированного сертификата ключа проверки электронной подписи	Субъект – получатель квалифицированного сертификата ключа проверки электронной подписи	Документ, на основании которого Удостоверяющий центр выдает электронную подпись
1.2.643.5.1.24.2.5	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель (заместитель руководителя) органа местного самоуправления по учету муниципального имущества или иное уполномоченное лицо данного органа в соответствии с федеральным законом	Документ, подтверждающий полномочия
1.2.643.5.1.24.2.6	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель органа государственной власти субъекта Российской Федерации или иное уполномоченное лицо данного органа в соответствии с федеральным законом	Документ, подтверждающий полномочия
1.2.643.5.1.24.2.8	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Судья	Документ, подтверждающий полномочия (только для Агентства по обеспечению деятельности мировых судей Красноярского края)
1.2.643.5.1.24.2.19	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель органа местного самоуправления или иное уполномоченное лицо данного органа в соответствии с федеральным законом	Документ, подтверждающий полномочия

1.2.643.5.1.24.2.44	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководитель (заместитель руководителя) органа исполнительной власти субъекта Российской Федерации по учету государственного имущества субъекта Российской Федерации или иное уполномоченное лицо данного органа в соответствии с федеральным законом	Документ, подтверждающий полномочия
1.2.643.5.1.24.2.49	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости	Руководители (заместители руководителей) многофункциональных центров предоставления государственных и муниципальных услуг	Документ, подтверждающий полномочия
1.2.643.5.1.24.2.53	Формирование запроса о предоставлении сведений из государственного кадастра недвижимости и о предоставлении общедоступных сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним	Руководитель подведомственной организации органа государственной власти субъекта Российской Федерации, участвующей в предоставлении государственных или муниципальных услуг, или иное уполномоченное лицо данной организации в соответствии с федеральным законом	Документ, подтверждающий полномочия
1.2.643.5.1.24.2.54	Формирование запроса о предоставлении сведений из государственного кадастра недвижимости и о предоставлении общедоступных сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним	Руководитель подведомственной организации органа местного самоуправления, участвующей в предоставлении государственных или муниципальных услуг, или иное уполномоченное лицо данной организации в соответствии с федеральным законом	Документ, подтверждающий полномочия

Приложение №11
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма соглашения о безвозмездном оказании услуг удостоверяющего центра***)

СОГЛАШЕНИЕ № _____
о безвозмездном оказании услуг удостоверяющего центра

г. Красноярск **«___» _____ 20__ г.**

Краевое государственное казённое учреждение «Центр информационных технологий Красноярского края», в лице, _____, действующего (ей) на основании доверенности от _____ №_____, именуемое в дальнейшем «Удостоверяющий центр», с одной стороны, и _____, в лице _____, действующего на основании _____ именуемое в дальнейшем «Абонент», с другой стороны, вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1.ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Абонент поручает, а Удостоверяющий центр принимает на себя обязательства по оказанию услуг удостоверяющего центра, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон) и Регламентом деятельности Удостоверяющего центра (далее – Регламент УЦ).

1.2. Абонент принимает условия оказания услуг Удостоверяющего центра, описанных в Регламенте УЦ, размещенном в сети Интернет по адресу: http://www.it.krskstate.ru/udostov_centr/reglament.pdf. Факт заключения настоящего Соглашения считается фактом присоединения к Регламенту УЦ, в порядке ст. 428 Гражданского кодекса РФ.

1.3. Для получения услуг Удостоверяющего центра Абонент представляет в Удостоверяющий центр следующие документы, заверенные руководителем Абонента:

- копию свидетельства о государственной регистрации Абонента в качестве юридического лица;
- копию свидетельства о присвоении Абоненту ИНН;
- копию приказа (протокола) о назначении руководителя Абонента;
- иные надлежащим образом оформленные заявительные документы, определенные пунктом 6.1 Регламента УЦ.

1.4. Основные термины, используемые в настоящем Соглашении, применяются в значениях, установленных Федеральным законом и Регламентом УЦ.

2.ОБЯЗАННОСТИ СТОРОН

2.1. Удостоверяющий центр обязан:

2.1.1. Обеспечивать формирование ключей электронных подписей (далее – ЭП) и осуществлять изготовление квалифицированных сертификатов ключей проверки ЭП (далее – СКПЭП) по обращению Абонента, с гарантией сохранения в тайне ключа ЭП в случае его генерации уполномоченным сотрудником Удостоверяющего центра.

2.1.2. Вести реестр изготовленных СКПЭП, обеспечивать его актуальность и возможность свободного доступа к нему.

2.1.3. Приостанавливать, возобновлять действие и аннулировать СКПЭП по обращению Абонента и его полномочных представителей (владельцев СКПЭП) в соответствии с Регламентом УЦ.

2.1.4. Выдавать квалифицированные СКПЭП в форме электронных документов и в форме документов на бумажных носителях.

2.1.5. Проводить работы при обращении Абонента по подтверждению подлинности ЭП в электронном документе в отношении СКПЭП, выданных Удостоверяющим центром.

2.1.6. При создании ключей ЭП и СКПЭП использовать сертифицированные в соответствии с законодательством Российской Федерации средства ЭП.

2.1.7. Уведомлять владельца СКПЭП о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования ключа ЭП.

2.1.8. Обеспечить хранение СКПЭП в форме электронного документа в течение трех лет.

2.1.9. Участвовать в разрешении конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением полученных электронных документов, а также с использованием в данных документах электронной подписи.

2.2. Абонент обязуется:

2.2.1. Обеспечить достоверность информации, идентифицирующей сотрудников Абонента - владельцев СКПЭП.

2.2.2. Обеспечить хранение в тайне ключей ЭП Пользователями УЦ (сотрудниками Абонента).

2.2.3. Обеспечить неиспользование ключей электронной подписи своими сотрудниками (Пользователями УЦ), если Пользователю УЦ стало известно, что его ключи используются или использовались посторонними лицами.

2.2.4. Немедленно требовать приостановления (прекращения) действия СКПЭП при наличии оснований полагать, что тайна ключа ЭП была нарушена, а также при отзыве доверенности, выданной сотруднику Абонента (Пользователю УЦ), или истечении срока её действия.

2.2.5. При взаимодействии с Удостоверяющим центром руководствоваться Регламентом Удостоверяющего центра. Не реже одного раза в 30 дней обращаться к web-сайту УЦ http://www.it.krskstate.ru/udostov_centr для ознакомления с оповещениями, а также изменениями Регламента УЦ.

2.2.6. При обращении со средствами ЭП руководствоваться требованиями эксплуатационной документации на них и нормативными документами, регламентирующими использование СКЗИ.

2.2.7. Обеспечить рабочее место, предназначенное для работы со средствами ЭП, лицензионным системным программным обеспечением и средствами антивирусной защиты.

2.2.8. Установить за свой счёт программное обеспечение, предназначенное для работы со средствами ЭП.

3.ПОРЯДОК ОКАЗАНИЯ УСЛУГ

3.1. Срок изготовления ключей ЭП и СКПЭП Удостоверяющим центром составляет не более 10 рабочих дней с даты поступления Заявки в Удостоверяющий центр.

3.2. Передача Абоненту СКПЭП осуществляется по адресу: г. Красноярск, ул. Робеспьера 32, пом. 176.

3.3. Порядок плановой и внеплановой смены ключей ЭП и СКПЭП, а также действия при компрометации ключей ЭП описан в Регламенте УЦ.

4.УСЛОВИЯ О КОНФИДЕНЦИАЛЬНОСТИ

4.1. Стороны обязуются не допускать разглашения конфиденциальных данных, ставших им известными в процессе исполнения настоящего Соглашения.

4.2. Обязательства Сторон относительно конфиденциальности и неразглашения информации не распространяются на информацию, имеющую статус открытой в соответствии с законодательством Российской Федерации.

4.3. Конфиденциальная информация, полученная одной из Сторон, может быть передана органам государственной власти Российской Федерации, по основаниям и в порядке, установленным законодательством Российской Федерации, с незамедлительным уведомлением об этом другой Стороны.

4.4. Запрет на разглашение конфиденциальной информации устанавливается без ограничения срока.

5.ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации и условиями настоящего Соглашения.

5.2. Сторона, не исполнившая своих обязательств вследствие действия обстоятельств непреодолимой силы, обязана в течение 5 рабочих дней письменно известить другую Сторону о начале и об окончании возникшего препятствия и его влиянии на исполнение условий настоящего Соглашения.

5.3. Если обстоятельства непреодолимой силы действуют на протяжении трех месяцев и не обнаруживают признаков прекращения, настоящее Соглашение может быть расторгнуто по соглашению Сторон без обязанности по возмещению убытков.

5.4. При несоблюдении обязанностей, изложенных в статье 10 Федерального закона 63-ФЗ, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

6.ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

6.1. Все споры и разногласия, возникающие между Сторонами при исполнении настоящего Соглашения, разрешаются путем переговоров.

6.2. Если спор не был разрешен Сторонами путем переговоров в течение 20 рабочих дней с момента направления одной Стороной другой Стороне уведомления о необходимости урегулирования спора или в любой другой согласованный Сторонами срок, спор может быть передан на рассмотрение Арбитражного суда Красноярского края.

7.СРОК ДЕЙСТВИЯ И ПОРЯДОК ИЗМЕНЕНИЯ СОГЛАШЕНИЯ

7.1. Настоящее Соглашение вступает в силу с момента его подписания и действует сроком один год. Действие настоящего соглашения автоматически пролонгируется если в реквизитах Сторон, в том числе в сведениях о подписанте, не произошло никаких изменений.

7.2. Все изменения настоящего Соглашения действительны и обязательны для исполнения Сторонами, если они оформлены в письменном виде и подписаны уполномоченными представителями Сторон, за исключением случаев, предусмотренных пунктом 7.3. настоящего Соглашения.

7.3. Изменения условий настоящего Соглашения и применяемых в связи с его исполнением документов, обусловленные изменением действующего законодательства, вступают с силу одновременно с вступлением в силу соответствующих правовых актов.

8.ПРОЧИЕ УСЛОВИЯ

8.1. Взаимоотношения Сторон, не урегулированные настоящим Соглашением, регламентируются действующим законодательством Российской Федерации.

8.2. Настоящее Соглашение составлено в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой Стороны.

8.3. Сторона в случае ее реорганизации либо изменения адреса, наименования, банковских реквизитов уведомляет об этом другую Сторону в письменном виде в течение 10 рабочих дней со дня реорганизации, изменения адреса, наименования, банковских реквизитов.

8.4. Услуги Удостоверяющего центра оказываются Абоненту на безвозмездной основе.

9.ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН

УДОСТОВЕРЯЮЩИЙ ЦЕНТР	**АБОНЕНТ**
Краевое государственное казённое учреждение «Центр информационных технологий Красноярского края» Адрес: 660021, г. Красноярск, ул. Робеспьера, 32, пом. 176 ИНН /КПП 2466226448 / 246001001 Банковские реквизиты р/с 40201810000000000003 БИК 040407001 в Отделении Красноярск г. Красноярск	

10. ПОДПИСИ СТОРОН

М.П. М.П.

Приложение №12
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Памятка владельцу сертификата ключа проверки электронной подписи по безопасности***)

ПАМЯТКА
владельцу сертификата ключа проверки электронной подписи по безопасности

1. Электронная подпись является аналогом собственноручной подписи владельца сертификата ключа проверки электронной подписи, с которым эта электронная подпись связана.
2. Подписание электронного документа или электронного сообщения электронной подписью осуществляется путем применения ключа электронной подписи к этому электронному документу (файлу) или электронному сообщению.
3. Применение ключа электронной подписи происходит путем обращения к контейнеру ключа электронной подписи. Обращение к контейнеру ключа электронной подписи осуществляет программа в момент подписания файла, сообщения, запроса или иного электронного документа электронной подписью, после того как подписант выбрал в процессе подписания свой сертификат ключа проверки электронной подписи. В случае если в «Личном хранилище» сертификатов в операционной системе автоматизированного рабочего места (АРМ) пользователя содержится только один сертификат ключа проверки электронной подписи, то система выбирает его автоматически, не предлагая пользователю выбрать требуемый сертификат ключа проверки электронной подписи в процессе подписания.
4. Ключ электронной подписи и пароль (или пин-код) доступа к контейнеру ключа электронной подписи являются закрытой (конфиденциальной) информацией, сертификат ключа проверки электронной подписи является открытой информацией. Персональные данные, включаемые в сертификат ключа проверки электронной подписи, являются общедоступными.
5. Для защиты ключа электронной подписи от несанкционированного использования применяется пароль доступа к контейнеру ключа электронной подписи (в случае хранения контейнера закрытого ключа на файловом носителе) либо пин-код доступа к ключевому носителю, если в качестве такового используется специализированное устройство типа eToken, RuToken, JaCarta и т.п. При получении ключевого носителя от Оператора УЦ рекомендуется самостоятельно сменить пароль на контейнер ключа электронной подписи. ***Забывать пароль не следует, иначе неизбежно необходимо будет проводить процедуру внеплановой смены ключа!***
6. Владелец сертификата ключа проверки электронной подписи и соответствующего ему ключа электронной подписи в целях предотвращения несанкционированного использования ключа электронной подписи обязан ***не допускать попадание носителя контейнера ключа электронной подписи к посторонним лицам, а также хранить в тайне пароль доступа к ключевому контейнеру (пин-код от ключевого носителя). Одной из обязательных мер по предотвращению хищения содержимого ключевого контейнера, а также перехвату пароля доступа к ключевому контейнеру, является антивирусная защита компьютера***, на котором осуществляется применение ключа электронной подписи.

7. Контейнер ключа электронной подписи может храниться на любом носителе, поддерживаемом программным обеспечением криптопровайдера. В целях обеспечения безопасности ключа электронной подписи ***рекомендуется контейнер ключа электронной подписи хранить на отчуждаемом электронном носителе***. Также настоятельно не рекомендуется при обращении к контейнеру закрытого ключа устанавливать пометку «Запомнить пароль».
8. В целях обеспечения доступности ключа проверки электронной подписи ***рекомендуется сделать резервную копию ключевого контейнера на другой отчуждаемый носитель, который хранить в сейфе*** или ином недоступном для посторонних лиц месте. В случае выхода из строя основного ключевого носителя, владелец ключа электронной подписи сможет воспользоваться резервной копией.
9. Чтобы «привязать» сертификат ключа проверки электронной подписи к ключевому контейнеру необходимо процедуру установки сертификата ключа проверки электронной подписи в хранилище «Личное» операционной системы компьютера пользователя ***провести средствами программного обеспечения криптопровайдера (например «КриптоПро CSP»)***. Эту же процедуру необходимо провести перед началом использования резервной копии ключа электронной подписи.
10. В случае компрометации ключа электронной подписи (т.е. фактов, связанных с вирусным заражением компьютера пользователя, с попаданием носителя ключа электронной подписи в посторонние руки, с подозрением о том, что пароль доступа к ключевому контейнеру стал известен посторонним лицам) следует прекратить использование скомпрометированного ключа электронной подписи и обратиться в Удостоверяющий центр с заявлением об отзыве или приостановлении действия сертификата ключа проверки электронной подписи.

Приложение №13
к Регламенту деятельности Краевого удостоверяющего центра
электронного правительства Красноярского края
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(***Форма согласия на обработку персональных данных***)

СОГЛАСИЕ
на обработку персональных данных[1]

Я, _____
(Фамилия, Имя, Отчество)

зарегистрированн_____ по адресу:
(ый/ая)

_____

документ, удостоверяющий личность: _____
Серия: _____ № _____
Выдан:

_____

Код подразделения: _____
Дата выдачи: _____

в соответствии с частью 4 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях получения квалифицированного сертификата ключа проверки электронной подписи даю Краевому государственному казенному учреждению «Центр информационных технологий Красноярского края» свое согласие на обработку, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение моих персональных данных, содержащихся в копии основного документа, удостоверяющего личность, а также иных документах, предоставленных для получения квалифицированного сертификата ключа проверки электронной подписи.

Настоящее согласие действует со дня его подписания до дня предоставления соответствующего отзыва в письменной форме.

"___"_____ ____ г. _____
(подпись и ФИО субъекта персональных данных)

[1] В соответствии с пунктом 2 части 4 статьи 9 Федерального закона от 05.10.2011 № 152-ФЗ «О персональных данных», при получении согласия от представителя субъекта персональных данных в Согласии на обработку персональных данных также указывается фамилия, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя.

Лист регистрации изменений

№ изменения	Номера листов (страниц)			Всего листов (страниц) в документе	Номер и дата приказа о внесении изменений в Регламент
	измененных	новых	аннулированных		
1.	все	все	все	52	Приказ №21 о.д. от 30 мая 2017
2.	все	0	0	55	Приказ №31 от 03 августа 2017
3	3-5, 7-10, 12, 14-25, 29, 30, 32, 34, 41, 42, 50, 52-55	0	0	55	Приказ №12 о.д. от 08 февраля 2018