

Утвержден
Приказом ООО «КРИПТО-ПРО»
от 02 ноября 2009 г. №2/11-09-УЦ

РЕГЛАМЕНТ
Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)

Редакция №4

г. Москва
2009

1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о регистрации № 001.602.749, выдано 16.11.1999г. Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003г., Свидетельство о внесении записи в ЕГРЮЛ в связи с государственной регистрацией изменений, вносимых в учредительные документы юридического лица за государственным регистрационным номером 2037719011031 от 12.03.2003г.

Удостоверяющий центр в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов открытых ключей осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1. **Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны N 6388Р от 30 ноября 2008 г. на право осуществления** распространения шифровальных (криптографических) средств;
2. **Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны N 6387Х от 30 ноября 2008 г. на право осуществления** технического обслуживания шифровальных (криптографических) средств;
3. **Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны N 6389У от 30 ноября 2008 г. на право предоставления услуг в области шифрования информации;**
4. **Лицензия ФСТЭК России 0439 от 02 февраля 2006 г. на деятельность по** технической защите конфиденциальной информации.

Сертификаты ключей подписей уполномоченного лица Удостоверяющего центра зарегистрированы Уполномоченным федеральным органом исполнительной власти Российской Федерации в части применения электронной цифровой подписи в Едином государственном реестре сертификатов уполномоченных лиц удостоверяющих центров, о чем получены соответствующие уведомления:

1. Уведомление № 32 от 06 апреля 2006 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Выдано Росинформтехнологии. Регистрационный номер записи П-44-05-12-19 от 23 января 2006 г.
2. Уведомление № 33 от 06 апреля 2006 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Выдано Росинформтехнологии. Регистрационный номер записи П-44-05-12-20 от 23 января 2006 г.

3. Уведомление № 56 от 06 июня 2006 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Выдано Росинформтехнологии. Регистрационный номер записи П-44-05-12-52 от 05 июня 2006 г.
4. Уведомление № 109 от 19 апреля 2007 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Выдано Росинформтехнологии. Регистрационный номер записи П-44-05-12-107 от 19 апреля 2007 г.;
5. Уведомление № 189 от 15 июля 2008 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Выдано Росинформтехнологии. Регистрационный номер записи П44-05-12-188 от 15 июля 2008 г.
6. Уведомление № 6 от 18 мая 2009 г. о внесении в Единый государственный реестр сертификатов ключей подписей удостоверяющих центров. Выдано Росинформтехнологии. Регистрационный номер записи П44-05-12-275 от 18 мая 2009 г.

Реквизиты ООО «КРИПТО-ПРО»:

Полное наименование: Общество с ограниченной ответственностью «КРИПТО-ПРО»

Юридический адрес: 105094, г. Москва, ул. Золотая д.11

Фактический адрес: 127018, г. Москва, ул. Суцевский вал, д. 16, стр. 5

Адрес для корреспонденции: 127018, г. Москва, А/Я «КРИПТО-ПРО» (б/н)

Банковские реквизиты (наименование банка, БИК, ИНН, р/с, к/с):

- Филиал ОАО "МДМ БАНК" г. Москва
- БИК 044525495
- Р/с 40702810100120035754
- К/с 30101810900000000495

ИНН/КПП: 7717107991/771901001

ОГРН: 1037700085444

Код по ОКВЭД: 73.10, 74.30, 74.14, 74.84, 72.20, 72.40, 72.60

Код по ОКПО: 51282566

Контактные телефоны, факс, адрес электронной почты:

- тел./факс (495) 780-48-20; e-mail: cpca@cryptopro.ru, info@cryptopro.ru

2. Термины и определения

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром расписываться собственноручной подписью в сертификатах ключей подписей на бумажном носителе, изданных Удостоверяющим центром

АРМ (автоматизированное рабочее место) Пользователя УЦ – web-приложение, предназначенное для регистрации и управления сертификатами ключей подписей Пользователя УЦ, размещенное на web-узле Удостоверяющего центра

База сертификатов Портала – совокупность данных, содержащихся в сертификатах Пользователей Доверенных Удостоверяющих центров и систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью программного обеспечения Участников Системы Портала

Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы)

Доверенный Удостоверяющий центр – удостоверяющий центр, сертификаты уполномоченных лиц которого включены в Реестр Портала

Единое пространство доверия сертификатам ключей подписей Портала – информационное пространство, в котором организационными и техническими мерами обеспечивается взаимное доверие сертификатам ключей подписей Участников портала, осуществляющееся на основе Реестра Доверенных Удостоверяющих центров Портала

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Закрытый ключ электронной цифровой подписи действует на определенный момент времени (действующий закрытый ключ) если:

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат ключа подписи, соответствующий данному закрытому ключу, действует на указанный момент времени.

Маркер временного доступа – идентификатор (десятичное число) и секретный пароль (пятизначное символьное значение), предоставляющиеся Пользователю УЦ, не имеющему действующего закрытого ключа, для

формирования и предоставления в Удостоверяющий центр запроса на сертификат ключа подписи посредством АРМ Пользователя УЦ

Оператор Портала – уполномоченное лицо организатора Системы «Портал доверенных услуг ФГУП НИИ «Восход», ответственное за ведение Реестра Портала, являющийся владельцем сертификата ключа подписи, изданным Удостоверяющим центром ФГУП НИИ «Восход»

Оператор Службы актуальных статусов сертификатов – ответственный сотрудник Удостоверяющего центра, являющийся владельцем сертификата ключа подписи и соответствующего закрытого ключа, с использованием которого подписываются электронной цифровой подписью электронные ответы Службы актуальных статусов сертификатов.

Оператор Службы штампов времени – ответственный сотрудник Удостоверяющего центра, являющийся владельцем сертификата ключа подписи и соответствующего закрытого ключа, с использованием которого подписываются электронной цифровой подписью штампы времени.

Организатор Портала - Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Восход»

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо (в случае присоединения к Регламенту юридического лица – уполномоченный представитель Стороны, присоединившейся к Регламенту), зарегистрированное в Удостоверяющем центре

Псевдоним владельца сертификата ключа подписи – вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре

Рабочий день Организатора системы Портала – промежуток времени с 10:00 по 18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней

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

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

- реестр заявлений о присоединении к Регламенту Удостоверяющего центра;
- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификатов ключей подписей;

- реестр заявлений на аннулирование (отзыв) сертификатов ключей подписей;
- реестр заявлений на приостановление/возобновление действия сертификатов ключей подписей;
- реестр заявлений на подтверждение подлинности электронной цифровой подписи в электронном документе;
- реестр сертификатов ключей подписей;
- реестр изготовленных списков отозванных сертификатов.

Сертификат ключа подписи - электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра или документ на бумажном носителе, подписанный собственноручной подписью уполномоченного на то лица Удостоверяющего центра и заверенный печатью Удостоверяющего центра, структура которого определяется настоящим Регламентом и который изготавливается Удостоверяющим центром для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

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

- наступил момент времени начала действия сертификата ключа подписи;
- срок действия сертификата ключа подписи не истек;
- сертификат ключа подписи не аннулирован (отозван) и действие его не приостановлено

Система «Портал доверенных услуг ФГУП НИИ «Восход» (Портал) - корпоративная информационная система, организатором которой является Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Восход», предназначенная для оказания услуг в области использования электронной цифровой подписи и телематических услуг связи, с использованием сертификатов ключей подписей, изданных удостоверяющими центрами, аттестованными в данной системе. Сайт Портала доверенных услуг – www.trustportal.ru

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

Средство электронной цифровой подписи – средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», обеспечивающее реализацию следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи

подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Удостоверяющий центр – ООО «КРИПТО-ПРО», осуществляющее выполнение целевых функций Удостоверяющего центра в соответствии с ФЗ «Об электронной цифровой подписи» от 10.01.2002 года и выполняющее следующие основные функции по управлению сертификатами ключей подписей:

- изготавливает сертификаты ключей подписей;
- создает закрытые ключи электронных цифровых подписей с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр Удостоверяющего центра, обеспечивает его актуальность;
- проверяет уникальность открытых ключей;
- выдает сертификаты ключей подписей с информацией об их действии;
- осуществляет подтверждение подлинности электронной цифровой подписи в электронном документе.

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов

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

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме

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

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

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

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует

описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;

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

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

3. Статус Регламента

3.1. Регламент Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров

3.2. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации

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

3.4. Настоящий регламент распространяется:

в форме электронного документа:

- по адресу: URL=<http://cpca.cryptopro.ru/reglament/reglamentdist.pdf>

в форме документа на бумажном носителе:

- при подаче Заявления о присоединении к Регламенту (за вознаграждение, установленное настоящим Регламентом)

4. Общие положения

4.1. Присоединение к Регламенту

4.1.1. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр Заявления о присоединении к Регламенту по форме Приложения № 1 настоящего Регламента

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

4.1.3. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления о присоединении к Регламенту

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

4.1.5. После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения на неопределённый срок

4.2. Порядок расторжения Регламента

4.2.1. Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

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

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

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

4.3. Изменение (дополнения) Регламента

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

4.3.2. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на сайте Удостоверяющего центра по адресу – <http://cpca.cryptopro.ru/reglament/reglamentdist.pdf>

4.3.3. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении двух месяцев с даты размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра по адресу - <http://cpca.cryptopro.ru/reglament/reglamentdist.pdf>

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

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

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

4.4. Применение Регламента

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

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

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

5. Предоставление информации

5.1. Удостоверяющий Центр предоставляет Стороне, присоединившейся к Регламенту, по ее требованию:

- копию лицензии ФСБ России на осуществление профессиональной деятельности по распространению шифровальных (криптографических средств);
- копию лицензии ФСБ России на осуществление профессиональной деятельности по техническому обслуживанию шифровальных (криптографических средств);
- копию лицензии ФСБ России на осуществление профессиональной деятельности на предоставление услуг в области шифрования информации;
- копию лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

5.2. Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить Удостоверяющему центру документы, подтверждающие следующую информацию:

Для юридических лиц:

- наименование организации и основной государственный регистрационный номер, идентификационный номер налогоплательщика;
- нотариально заверенную копию Устава организации; нотариально заверенную копию учредительного договора (если есть);
- нотариально заверенную копию свидетельства ИМНС о государственной регистрации;
- копии протоколов, либо иных документов, о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и/или надлежащим образом оформленные доверенности;
- сведения, необходимые для идентификации полномочного представителя организации: фамилия, имя, отчество, номер паспорта, дата и кем выдан, место регистрации.

Для физических лиц:

- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность.

6. Права и обязанности сторон

6.1. Удостоверяющий центр обязан:

6.1.1. Предоставить Пользователю Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра

6.1.2. Использовать для изготовления закрытого ключа уполномоченного лица Удостоверяющего центра и формирования электронной цифровой подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной цифровой подписи.

6.1.3. Использовать закрытый ключ уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей подписей и списков отозванных сертификатов

6.1.4. Принять меры по защите закрытого ключа уполномоченного лица Удостоверяющего центра от несанкционированного доступа

6.1.5. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Москвы. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности

6.1.6. Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте

6.1.7. Обеспечить занесение регистрационной информации Пользователя Удостоверяющего центра в Реестр Удостоверяющего центра и обеспечить уникальность регистрационной информации всех зарегистрированных в Удостоверяющем центре лиц, используемой для идентификации владельцев сертификатов ключей подписей

6.1.8. Изготовить сертификат ключа подписи зарегистрированного в Удостоверяющем центре пользователя по заявлению на изготовление сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте

6.1.9. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей подписей

6.1.10. Обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей подписей пользователей Удостоверяющего центра

6.1.11. Аннулировать (отозвать), приостановить и возобновить действие сертификата ключа подписи Пользователя Удостоверяющего центра по соответствующему заявлению на аннулирование (отзыв), приостановление и возобновление действия сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте

6.1.12. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра, если истек установленный срок, на который действие данного сертификата было приостановлено.

6.1.13. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра в случае компрометации закрытого ключа уполномоченного лица Удостоверяющего центра, с использованием которого был издан сертификат ключа подписи.

6.1.14. Официально уведомить об аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключа подписи всех лиц, зарегистрированных в Удостоверяющем центре

6.1.15. Публиковать актуальный список отозванных сертификатов на сайте Удостоверяющего центра в ресурсе: <http://cpca.cryptopro.ru/ra/cdp/>. Период публикации списка отозванных сертификатов в рабочее время Удостоверяющего центра – 1 час

6.1.16. Обеспечить соответствие программно-аппаратной реализации и организационно-правовых мер требованиям Портала, определенным в «Положении о порядке аттестации Удостоверяющих центров в системе «Портал доверенных услуг ФГУП НИИ «Восход» и «Требованиям к средствам криптографической защиты информации и сертификатам открытых ключей ЭЦП, используемым в системе «Портал доверенных услуг «ФГУП НИИ Восход».

6.1.17. Обеспечить занесение всех выпущенных сертификатов ключей подписей Пользователей Портала в Базу сертификатов Портала путем передачи информации Организатору Портала не позднее рабочего дня Организатора Портала следующего за днем выпуска сертификата ключа подписи, предназначенного для использования в системе Портала.

6.2. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1. Известить Удостоверяющий центр об изменениях в документах, приведенных в п.5.2. и по требованию Удостоверяющего центра предоставить их в течение 5-ти рабочих дней с момента регистрации изменений

6.2.2. С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу <http://cpca.cryptopro.ru/reglament/reglamentdist.pdf> за сведениями об изменениях и дополнениях в Регламент

6.2.3. Пользователь Удостоверяющего центра обязан:

6.2.3.1. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования

6.2.3.2. Применять для формирования электронной цифровой подписи только действующий личный закрытый ключ

6.2.3.3. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами

6.2.3.4. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи (расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи)

6.2.3.5. Немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если Пользователю

Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами

6.2.3.6. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата по момент времени официального уведомления об аннулировании (отзыве) сертификата

6.2.3.7. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата по момент времени официального уведомления о приостановлении действия сертификата

6.2.3.8. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован (отозван) или действие его приостановлено

6.2.3.9. Не использовать личный закрытый ключ до предоставления Удостоверяющему центру подписанной копии сертификата ключа подписи, соответствующего данному закрытому ключу

6.3. Удостоверяющий центр имеет право:

6.3.1. Отказать пользователю в регистрации в Удостоверяющем центре в случае ненадлежащего оформления необходимых регистрационных документов

6.3.2. Отказать в изготовлении сертификата ключа подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи

6.3.3. Отказать в аннулировании (отзыве) сертификата ключа подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа подписи

6.3.4. Отказать в приостановлении/возобновлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата ключа подписи

6.3.5. Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату

6.3.6. Отказать в приостановлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату

6.3.7. Отказать в возобновлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату

6.3.8. Отказать в изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа подписи

средство криптографической защиты информации (средство электронной цифровой подписи) не поддерживается Удостоверяющим центром.

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

6.4. Пользователь Удостоверяющего центра имеет право:

6.4.1. Применять сертификат ключа подписи уполномоченного лица Удостоверяющего центра для проверки электронной цифровой подписи уполномоченного лица Удостоверяющего центра в сертификатах ключей подписей, изготовленных Удостоверяющим центром

6.4.2. Применять список отозванных сертификатов ключей подписей, изготовленный Удостоверяющим центром, для установления статуса сертификатов ключей подписей, изготовленных Удостоверяющим центром

6.4.3. Применять сертификат ключа подписи Пользователя Удостоверяющего центра для проверки электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи

6.4.4. Для хранения личного закрытого ключа применять носитель, поддерживаемый средством электронной цифровой подписи

6.4.5. Обратиться в Удостоверяющий центр с заявлением на изготовление сертификата ключа подписи.

6.4.6. Обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) и приостановление действия сертификата ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

6.4.7. Обратиться в Удостоверяющий центр с заявлением на возобновление действия сертификата ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа и срока, на который действие сертификата было приостановлено.

6.4.8. Обратиться в Удостоверяющий центр за получением информации о статусе сертификатов ключей подписей и их действительности на определенный момент времени.

6.4.9. Обратиться в Удостоверяющий центр за подтверждением подлинности ЭЦП в электронном документе, сформированной с использованием сертификата ключа подписи, изданного Удостоверяющим центром.

6.4.10. Воспользоваться доступом к системе «Портал доверенных услуг «ФГУП НИИ Восход» в том случае, если данный пользователь является владельцем сертификата, использующимся в указанной системе.

6.4.11. Воспользоваться дополнительными услугами системы «Портал доверенных услуг «ФГУП НИИ Восход» путем заключения договора на оказание дополнительных услуг с Организатором Портала. Информация о дополнительных услугах Портала доступна на сайте Портала.

7. Вознаграждение Удостоверяющего центра. Сроки и порядок расчетов

7.1. Вознаграждение Удостоверяющего центра за изготовление Регламента Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) в бумажной форме составляет 600 (Шестьсот) рублей 00 копеек, включая НДС (18%) – 91 (Девяносто один) рубль 53 копейки.

7.2. Вознаграждение Удостоверяющего центра за изготовление сертификата ключа подписи (клиентский сертификат ключа подписи, структура которого определена пунктом 11.2 настоящего Регламента) составляет 3 500 (Три тысячи пятьсот) рублей 00 копеек, включая НДС (18%) – 533 (Пятьсот тридцать три) рубль 90 копеек, за каждый изготовленный сертификат ключа подписи.

7.3. Вознаграждение Удостоверяющего центра за изготовление сертификата ключа подписи (клиентский сертификат ключа подписи, структура которого определена пунктом 11.2 настоящего Регламента), обеспечивающего возможность установления статуса сертификата ключа подписи посредством сервиса Службы актуальных статусов сертификатов и получения штампов времени посредством сервиса Службы штампов времени составляет 4 000 (Четыре тысячи) рублей 00 копеек, включая НДС (18%) – 610 (Шестьсот десять) рублей 17 копеек, за каждый изготовленный сертификат ключа подписи.

7.4. Вознаграждение Удостоверяющего центра за изготовление сертификата ключа подписи (клиентский сертификат ключа подписи, структура которого определена пунктом 11.2 настоящего Регламента), обеспечивающего возможность работы в Системе «Портал доверенных услуг ФГУП НИИ «Восход» составляет 4 500 (Четыре тысячи пятьсот) рублей 00 копеек, включая НДС (18%) – 686 (Шестьсот восемьдесят шесть) рублей 44 копейки, за каждый изготовленный сертификат ключа подписи.

7.5. Вознаграждение Удостоверяющего центра за изготовление сертификата ключа подписи (серверный сертификат ключа подписи, структура которого определена пунктом 11.3 настоящего Регламента) составляет 10 000 (Десять тысяч) рублей 00 копеек, включая НДС (18%) – 1525 (Одна тысяча пятьсот двадцать пять) рубль 42 копейки, за каждый изготовленный сертификат ключа подписи.

7.6. Стоимость услуг Удостоверяющего центра, связанных с подтверждением подлинности ЭЦП одного электронного документа, формат которого соответствует требованиям настоящего Регламента и подписанного ЭЦП на сертификате ключа подписи, изданном Удостоверяющим центром, составляет 2 550 (Две тысячи пятьсот пятьдесят) рублей 00 копеек, включая НДС (18%) – 388 (триста восемьдесят восемь) рублей 98 копеек.

7.7. Предоставление услуг по изготовлению Регламента, изготовлению сертификатов ключей подписей, подтверждению подлинности ЭЦП в электронном документе осуществляется Удостоверяющим центром после оплаты соответствующего счета, выставленного Стороне, присоединившейся к Регламенту.

7.8. Изготовление сертификатов ключей подписей, вызванных внеплановой сменой ключей Пользователей УЦ, связанной с компрометацией ключей уполномоченного лица Удостоверяющего центра (пункт 12.2 настоящего Регламента), осуществляется Удостоверяющим центром безвозмездно.

8. Ответственность сторон

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

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

8.3. Удостоверяющий центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях Пользователя Удостоверяющего центра

8.4. Удостоверяющий центр несет ответственность за убытки при использовании закрытого ключа подписи и сертификата ключа подписи Пользователя Удостоверяющего центра только в случае, если данные убытки возникли при компрометации закрытого ключа уполномоченного лица Удостоверяющего центра

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

9. Разрешение споров

9.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к Регламенту

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

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

9.4. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы

9.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде города Москвы

10. Порядок предоставления и пользования услугами Удостоверяющего центра

10.1. Регистрация пользователя в Удостоверяющем центре и изготовление первого сертификата ключа подписи

Удостоверяющий центр осуществляет регистрацию физических и уполномоченных представителей юридических лиц только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с пунктом 4.1. настоящего Регламента.

Регистрация Пользователя в Удостоверяющем центре и изготовление первого сертификата ключа подписи осуществляется посредством web-интерфейса, предоставляемого Удостоверяющим центром, либо на основании файла запроса на сертификат ключа подписи.

10.1.1. Регистрация пользователя в Удостоверяющем центре и изготовление первого сертификата ключа подписи посредством web-интерфейса

Регистрация пользователя в Удостоверяющем центре осуществляется на основании заявления на регистрацию по форме Приложения №2 настоящего Регламента. Пользователь, являющийся уполномоченным представителем Стороны, присоединившейся к Регламенту (если Сторона Регламента - юридическое лицо), должен предоставить доверенность, выданную на его имя по форме Приложения №3 настоящего Регламента. Заявление на регистрацию и доверенность предоставляются в Удостоверяющий центр посредством почтовой либо курьерской связи.

После принятия положительного решения о регистрации Удостоверяющий центр предоставляет пользователю сертификат ключа подписи уполномоченного лица Удостоверяющего центра и сообщает адрес web-страницы регистрации в Удостоверяющем центре. Способ предоставления сертификата уполномоченного лица Удостоверяющего центра определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

Пользователь с помощью автоматизированного рабочего места (АРМ) пользователя Удостоверяющего центра формирует и направляет запрос на регистрацию в электронной форме в Удостоверяющий центр.

Ответственное лицо Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на регистрацию с информацией содержащейся в запросе на регистрацию, поданном в электронной форме. В случае идентичности указанной информации ответственное лицо Удостоверяющего центра регистрирует пользователя.

Регистрация пользователя и уведомление пользователя о регистрации должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого был подан запрос на регистрацию в Удостоверяющий центр в электронном виде.

После получения уведомления о регистрации в Удостоверяющем центре пользователь с помощью АРМ пользователя Удостоверяющего центра генерирует пару ключей, формирует и направляет запрос на сертификат ключа подписи в электронной форме в Удостоверяющий центр и подает заявление на изготовление сертификата по форме Приложения № 4 настоящего Регламента. Подача заявления осуществляется посредством почтовой либо курьерской связи.

После поступления заявления в Удостоверяющий центр ответственное лицо Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на изготовление сертификата с информацией, указанной в запросе на сертификат, поданном в электронной форме, и принимает решение об изготовлении сертификата ключа подписи.

В случае отказа в изготовлении сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра изготавливает сертификат ключа подписи.

Изготовление сертификата и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого было получено Заявление на изготовление сертификата ключа подписи в бумажной форме.

После получения уведомления об изготовлении сертификата пользователь с помощью АРМ пользователя Удостоверяющего центра вводит секретную ключевую фразу (данная фраза используется для аутентификации пользователя в Удостоверяющем центре при выполнении регламентных процедур, возникающих при компрометации ключевых документов), производит установку сертификата на своем рабочем месте и подтверждает ее.

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

10.1.2. Регистрация пользователя в Удостоверяющем центре и изготовление первого сертификата ключа подписи на основании файла запроса на сертификат

Регистрация пользователя в Удостоверяющем центре и изготовление первого сертификата ключа подписи осуществляется на основании заявления на регистрацию по форме Приложения №2 и заявления на изготовление сертификата по форме Приложения № 5 настоящего Регламента. Пользователь, являющийся уполномоченным представителем Стороны, присоединившейся к Регламенту (если Сторона Регламента - юридическое лицо), должен предоставить доверенность, выданную на его имя по форме Приложения №3 настоящего Регламента.

Заявление на регистрацию, заявление на изготовление сертификата и доверенность предоставляются в Удостоверяющий центр посредством почтовой либо курьерской связи. Способ предоставления файла запроса на сертификат ключа подписи (файл формата PKCS#10 в кодировке Base64) определяется регистрирующимся лицом по согласованию с Удостоверяющим центром.

После предоставления необходимых регистрационных документов и данных ответственное лицо Удостоверяющего центра осуществляет сравнение содержимого файла запроса на сертификат с данными, указанными в заявлении на изготовление сертификата и принимает решение о регистрации и об изготовлении первого сертификата ключа подписи.

В случае отказа в регистрации и изготовлении сертификата ключа подписи пользователь уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра регистрирует пользователя, изготавливает и предоставляет сертификат ключа подписи пользователю УЦ. Способ предоставления сертификата определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

Регистрация пользователя и изготовление сертификата ключа подписи должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого был предоставлен полный комплект регистрационных документов (заявление на регистрацию, доверенность, файл запроса на сертификат).

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

Дополнительно пользователю предоставляется сертификат уполномоченного лица Удостоверяющего центра и сообщается ключевая фраза, используемая для аутентификации пользователя при выполнении регламентных процедур, возникающих при компрометации ключевых документов. Способ предоставления сертификата уполномоченного лица Удостоверяющего центра и ключевой фразы определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

10.2. Изготовление сертификата ключа подписи Пользователя УЦ при плановой смене ключей

Изготовление сертификата ключа подписи при плановой смене ключей осуществляется посредством web-интерфейса, предоставляемого Удостоверяющим центром, либо на основании файла запроса на сертификат ключа подписи.

10.2.1. Изготовление сертификата ключа подписи при плановой смене ключей посредством web-интерфейса

Изготовление сертификата ключа подписи при плановой смене ключей осуществляется на основании заявления на изготовление сертификата, формируемого с использованием АРМ пользователя Удостоверяющего центра.

Заявление на изготовление сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата CMS. В качестве подписываемых данных используется запрос на сертификат ключа подписи в формате PKCS#10, а электронно-цифровая подпись осуществляется на действующем закрытом ключе Пользователя УЦ.

Значение поля Subject, содержащееся в запросе на сертификат, должно быть идентично значению этого поля в сертификате ключа подписи, соответствующему закрытому ключу Пользователя УЦ, на котором сформирована электронная цифровая подпись на заявлении на изготовление сертификата ключа подписи Пользователя УЦ.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Удостоверяющего центра принимает по нему решение.

В случае отказа в изготовлении сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра осуществляет изготовление сертификата ключа.

Изготовление сертификата ключа подписи и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого было получено и зарегистрировано в Удостоверяющем центре заявление на изготовление сертификата ключа подписи.

После получения уведомления об изготовлении сертификата пользователь с помощью АРМ пользователя Удостоверяющего центра производит установку сертификата на своем рабочем месте и подтверждает ее.

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

10.2.2. Изготовление сертификата ключа подписи при плановой смене ключей на основании файла запроса на сертификат

Изготовление сертификата ключа подписи при плановой смене ключей на основании файла запроса на сертификат осуществляется на основании заявления в электронной форме, либо на основании заявления в бумажной форме.

Заявление на изготовление сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата CMS. В качестве подписываемых данных используется запрос на сертификат ключа подписи в формате PKCS#10, а электронная цифровая подпись осуществляется на действующем закрытом ключе Пользователя УЦ.

Значение поля Subject, содержащееся в запросе на сертификат, должно быть идентично значению этого поля в сертификате ключа подписи, соответствующему закрытому ключу Пользователя УЦ, на котором сформирована электронная цифровая подпись на заявлении на изготовление сертификата ключа подписи Пользователя УЦ.

Формирование заявления в электронной форме на изготовление сертификата ключа подписи должно осуществляться средством, поддерживаемым Удостоверяющим центром (Приложение командной строки **cryptcp** (разработчик ООО «КРИПТО-ПРО»), приложение КриптоАРМ (разработчик ООО «Цифровые технологии»), почтовые клиенты Microsoft Outlook и Microsoft Outlook Express). Выбор конкретного средства формирования Заявления и способ его предоставления

определяется Пользователем УЦ по обязательному согласованию с Удостоверяющим центром.

После предоставления заявления в Удостоверяющий центр ответственный сотрудник Удостоверяющего центра принимает по нему решение.

В случае отказа в изготовлении сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра осуществляет изготовление и предоставление Пользователю УЦ сертификата ключа подписи. Способ предоставления сертификата определяется Пользователем УЦ по обязательному согласованию с Удостоверяющим центром.

Изготовление сертификата ключа подписи и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого было получено и зарегистрировано в Удостоверяющем центре заявление на изготовление сертификата ключа подписи.

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

Заявление в бумажной форме предоставляется в Удостоверяющий центр по форме Приложения №5 к настоящему Регламенту посредством почтовой либо курьерской связи. Дополнительно Пользователь УЦ предоставляет в Удостоверяющий центр файл запроса на сертификат ключа подписи. Запрос на сертификат ключа подписи должен соответствовать формату PKCS#10, представлен в кодировке Base64 с заголовком, порядок следования компонент имени субъекта совместим с порядком, установленным в Удостоверяющем центре. Способ предоставления файла запроса на сертификат ключа подписи определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

После предоставления необходимых документов и данных ответственное лицо Удостоверяющего центра осуществляет сравнение содержимого файла запроса на сертификат с данными, указанными в заявлении на изготовление сертификата и принимает решение об изготовлении сертификата ключа подписи.

В случае отказа в изготовлении сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра изготавливает сертификат ключа подписи.

Изготовление сертификата ключа подписи и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого был предоставлен полный комплект документов (заявление на изготовление сертификата, файл запроса на сертификат).

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

10.3. Изготовление сертификата ключа подписи Пользователя УЦ при внеплановой смене ключей

Внеплановая смена ключей осуществляется пользователем в следующих случаях:

- При компрометации закрытого ключа пользователя Удостоверяющего центра;
- При компрометации закрытого ключа уполномоченного лица Удостоверяющего центра;
- В случае, если пользователь по каким-либо причинам не смог осуществить плановую смену ключей в установленные для этой процедуры сроки;
- В иных случаях, вызванных форс-мажорными обстоятельствами

Изготовление сертификата ключа подписи при внеплановой смене ключей осуществляется посредством web-интерфейса, предоставляемого Удостоверяющим центром, либо на основании запроса на сертификат ключа подписи.

10.3.1. Изготовление сертификата ключа подписи Пользователя УЦ при внеплановой смене ключей посредством web-интерфейса

При наступлении события, повлекшего необходимость осуществления внеплановой смены ключей, Пользователь УЦ связывается по телефону с Удостоверяющим центром, и сообщает о необходимости проведения внеплановой смены ключей. Аутентификация пользователя осуществляется по ключевой фразе (секретному паролю), полученному пользователем при регистрации в Удостоверяющем центре.

В случае проведения успешной аутентификации, ответственное лицо Удостоверяющего центра формирует для пользователя «Маркер временного доступа». «Маркер временного доступа» предоставляется Пользователю УЦ. Способ предоставления определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

После получения «Маркера временного доступа» Пользователь УЦ с помощью АРМ пользователя Удостоверяющего центра генерирует пару ключей, формирует и направляет запрос на сертификат ключа подписи в электронной форме в Удостоверяющий центр и подает заявление на изготовление сертификата по форме Приложения №4 настоящего Регламента. Подача заявления осуществляется посредством почтовой либо курьерской связи.

После поступления заявления в Удостоверяющий центр ответственное лицо Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на изготовление сертификата с информацией, указанной в запросе на сертификат, поданном в электронной форме, и принимает решение об изготовлении сертификата ключа подписи.

В случае отказа в изготовлении сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра изготавливает сертификат ключа подписи.

Изготовление сертификата и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого было получено Заявление на изготовление сертификата ключа подписи в бумажной форме.

После получения уведомления об изготовлении сертификата пользователь с помощью АРМ пользователя Удостоверяющего центра производит установку сертификата на своем рабочем месте и подтверждает ее.

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

10.3.2. Изготовление сертификата ключа подписи Пользователя УЦ при внеплановой смене ключей на основании файла запроса на сертификат

Изготовление сертификата ключа подписи при внеплановой смене ключей на основании запроса на сертификат осуществляется на основании заявления в бумажной форме.

Заявление в бумажной форме предоставляется в Удостоверяющий центр по форме Приложения №5 к настоящему Регламенту посредством почтовой либо курьерской связи. Дополнительно Пользователь УЦ предоставляет в Удостоверяющий центр файл запроса на сертификат ключа подписи. Запрос на сертификат ключа подписи должен соответствовать формату PKCS#10, представлен в кодировке Base64 с заголовком, порядок следования компонент имени субъекта совместим с порядком, установленным в Удостоверяющем центре. Способ предоставления файла запроса на сертификат ключа подписи определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

После предоставления необходимых документов и данных ответственное лицо Удостоверяющего центра осуществляет сравнение содержимого файла запроса на сертификат с данными, указанными в заявлении на изготовление сертификата и принимает решение об изготовлении сертификата ключа подписи.

В случае отказа в изготовлении сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра изготавливает сертификат ключа подписи.

Изготовление сертификата ключа подписи и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3-х рабочих дней следующих за рабочим днем, в течение которого был предоставлен полный комплект документов (заявление на изготовление сертификата, файл запроса на сертификат).

После изготовления сертификата ключа подписи ответственный сотрудник Удостоверяющего центра формирует две копии сертификата, которые визируются уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Пользователю Удостоверяющего центра.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и соответствующим образом заверить две копии сертификата ключа подписи и предоставить в Удостоверяющий центр одну копию.

10.4. Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра

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

- в случае прекращения действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту;
- в случае отзыва доверенности Пользователя Удостоверяющего центра;
- по истечении срока, на который действие сертификата было приостановлено;
- по заявлению Пользователя Удостоверяющего центра;
- по истечении срока его действия;
- при компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра.

В случае прекращения действия настоящего Регламента, отзыва доверенности Пользователя, истечения срока, на который действие сертификата ключа подписи было приостановлено, отзыва сертификата Пользователя по его заявлению Удостоверяющий центр должен официально уведомить Пользователя и всех лиц, зарегистрированных в Удостоверяющем центре, об аннулировании (отзыве) сертификата не позднее одного рабочего дня с момента наступления описанного события.

Официальным уведомлением о факте отзыва сертификата ключа подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем отзыва сертификата ключа подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

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

В случае аннулирования сертификата ключа подписи Пользователя Удостоверяющего центра по истечении срока его действия временем аннулирования сертификата ключа подписи Пользователя Удостоверяющего центра признается время, хранящееся в поле notAfter поля Validity сертификата ключа подписи. В данном случае информация об аннулированном сертификате ключа подписи Пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра временем аннулирования сертификата ключа подписи Пользователя Удостоверяющего центра признается время компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра, фиксирующееся в реестре Удостоверяющего центра. В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра информация о сертификате ключа подписи Пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

Аннулирование (отзыв) сертификата ключа подписи осуществляется по заявлению его владельца, подающемуся в Удостоверяющий центр в электронной или бумажной форме, либо по заявлению Стороны, присоединившейся к Регламенту (если Сторона Регламента – юридическое лицо) на отзыв доверенности Пользователя Удостоверяющего центра.

10.4.1. Аннулирование (отзыв) сертификата ключа подписи Пользователя УЦ на основании заявления в электронной форме

Подача Пользователем УЦ заявления на аннулирование (отзыв) сертификата ключа подписи в электронной форме осуществляется с использованием АРМ пользователя Удостоверяющего центра.

Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата CMS. В качестве подписываемых данных используется запрос на отзыв сертификата ключа подписи, а электронная цифровая подпись осуществляется на действующем закрытом ключе Пользователя УЦ.

Запрос на отзыв сертификата ключа подписи представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер отзываемого сертификата ключа подписи;
- ReasonCode - код причины отзыва из следующего перечня допустимых значений:
 - o "0" Не указана
 - o "1" Компрометация ключа
 - o "2" Компрометация ЦС
 - o "3" Изменение принадлежности
 - o "4" Сертификат заменен
 - o "5" Прекращение работы

- SomeComment - текстовое значение комментария владельца сертификата ключа подписи.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Удостоверяющего центра принимает по нему решение.

В случае отказа в аннулировании (отзыве) сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра осуществляет аннулирование (отзыв) сертификата ключа.

Аннулирование (отзыв) сертификата ключа подписи и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата ключа подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было зарегистрировано заявление в Удостоверяющем центре.

10.4.2. Аннулирование (отзыв) сертификата ключа подписи Пользователя УЦ на основании заявления в бумажной форме

Заявление в бумажной форме предоставляется в Удостоверяющий центр по форме Приложения №6 к настоящему Регламенту посредством почтовой либо курьерской связи.

После предоставления заявления ответственное лицо Удостоверяющего центра принимает решение об аннулировании (отзыве) сертификата ключа подписи.

В случае отказа в аннулировании (отзыве) сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра осуществляет аннулирование (отзыв) сертификата ключа.

Аннулирование (отзыв) сертификата ключа подписи и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата ключа подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было зарегистрировано заявление в Удостоверяющем центре.

10.4.3. Аннулирование (отзыв) сертификата ключа подписи Пользователя УЦ на основании заявления на отзыв доверенности

Сторона, присоединившаяся к Регламенту, являющаяся юридическим лицом, вправе аннулировать (отозвать) сертификаты ключей подписей своих полномочных представителей, зарегистрированных в Удостоверяющем центре.

Аннулирование (отзыв) сертификатов ключей подписей Пользователей УЦ, являющихся полномочными представителями Стороны, присоединившейся к Регламенту, осуществляется путем отзыва доверенности, на основании которой Пользователю УЦ предоставлялись услуги Удостоверяющего центра. Форма заявления на отзыв доверенности приведена в Приложении №7 к настоящему Регламенту.

Аннулирование (отзыв) сертификата ключа подписи и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата ключа подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было зарегистрировано заявление на отзыв доверенности в Удостоверяющем центре.

10.5. Приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра

Удостоверяющий центр приостанавливает действие сертификата ключа подписи Пользователя Удостоверяющего центра в следующих случаях:

- по заявлению Пользователя Удостоверяющего центра в бумажной форме;
- по заявлению Пользователя Удостоверяющего центра в устной форме в случае компрометации или подозрения в компрометации закрытого ключа Пользователя Удостоверяющего центра;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

Действие сертификата ключа подписи приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа подписи составляет 10 (Десять) дней.

Если в течение срока приостановления действия сертификата ключа подписи действие этого сертификата не будет возобновлено, то сертификат ключа подписи аннулируется (отзывается) Удостоверяющим центром.

Приостановление действия сертификата ключа подписи и официальное уведомление Пользователя УЦ о приостановлении действия сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было принято заявление Удостоверяющим центром.

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

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

Приостановление действия сертификата ключа подписи осуществляется по заявлению его владельца, подающемуся в Удостоверяющий центр в устной, электронной или бумажной форме, а также по решению Удостоверяющего центра в случаях, определенных настоящим Регламентом.

10.5.1. Приостановление действия сертификата ключа подписи Пользователя УЦ на основании заявления в устной форме

Приостановление действия сертификата ключа подписи по заявлению Пользователя Удостоверяющего центра в устной форме осуществляется исключительно при компрометации закрытого ключа или подозрении в компрометации закрытого ключа Пользователя Удостоверяющего центра.

Заявление в устной форме подается в Удостоверяющий центр по телефону.

Заявитель должен сообщить ответственному сотруднику Удостоверяющего центра следующую информацию:

- идентификационные данные владельца сертификата ключа подписи;
- серийный номер сертификата ключа подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа подписи;
- ключевую фразу Пользователя УЦ (ключевая фраза определяется в процессе регистрации Пользователя УЦ).

Заявление принимается только в случае положительной аутентификации Пользователя УЦ (совпадения ключевой фразы переданной в заявлении с информацией из реестра пользователей Удостоверяющего центра).

После принятия заявления ответственный сотрудник Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа подписи.

В случае отказа в приостановлении действия сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра приостанавливает действие сертификата ключа подписи.

10.5.2. Приостановление действия сертификата ключа подписи Пользователя УЦ на основании заявления в электронной форме

Подача Пользователем УЦ заявления на приостановление действия сертификата ключа подписи в электронной форме осуществляется с использованием АРМ пользователя Удостоверяющего центра.

Заявление на приостановление действия сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата CMS. В качестве подписываемых данных используется запрос на приостановление действия сертификата ключа подписи, а электронная цифровая подпись осуществляется на действующем закрытом ключе Пользователя УЦ.

Запрос на приостановление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, HD=HoldDuration, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер сертификата открытого ключа, действие которого требуется приостановить;
- ReasonCode – «6» – приостановление действия;
- HoldDuration – срок, на который приостанавливается действие сертификата, в следующем формате: Y-M-W-D-H-M, где:
Y – число лет;
M – число месяцев;
W – число недель;
D – число дней;
H – число часов;
M – число минут;
- SomeComment - текстовое значение комментария владельца сертификата ключа подписи.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Удостоверяющего центра принимает по нему решение.

В случае отказа в приостановлении действия сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра приостанавливает действие сертификата ключа подписи.

10.5.3. Приостановление действия сертификата ключа подписи Пользователя УЦ на основании заявления в бумажной форме

Заявление в бумажной форме предоставляется в Удостоверяющий центр по форме Приложения №8 к настоящему Регламенту посредством почтовой либо курьерской связи.

После предоставления заявления ответственное лицо Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа подписи.

В случае отказа в приостановлении действия сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра приостанавливает действие сертификата ключа подписи.

10.5.4. Приостановление действия сертификата ключа подписи по решению Удостоверяющего центра

Удостоверяющий центр вправе приостановить действие сертификата ключа подписи Пользователя Удостоверяющего центра в случаях компрометации или подозрения в компрометации закрытого ключа подписи Пользователя Удостоверяющего центра в том случае, если Пользователю Удостоверяющего центра не было известно о возможном факте компрометации ключей, а также в случаях неисполнения обязательств Пользователя Удостоверяющего центра по настоящему Регламенту.

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

10.6. Возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра

Возобновление действия сертификата ключа подписи может быть осуществлено исключительно в период приостановления действия сертификата ключа подписи.

Возобновление действия сертификата ключа подписи и официальное уведомление Пользователя УЦ о возобновлении действия сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было принято заявление Удостоверяющим центром.

Официальным уведомлением о факте возобновления действия сертификата ключа подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления

действия сертификата ключа подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей в расширение CRL Distribution Point.

Возобновление действия сертификата ключа подписи осуществляется на основании заявления в электронной или бумажной форме.

10.6.1. Возобновление действия сертификата ключа подписи Пользователя УЦ на основании заявления в электронной форме

Подача Пользователем УЦ заявления на возобновление действия сертификата ключа подписи в электронной форме осуществляется с использованием АРМ пользователя Удостоверяющего центра.

Заявление на возобновление действия сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата CMS. В качестве подписываемых данных используется запрос на возобновление действия сертификата ключа подписи, а электронная цифровая подпись осуществляется на действующем закрытом ключе Пользователя УЦ.

Запрос на возобновление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер сертификата ключа подписи, действие которого требуется возобновить;
- ReasonCode – «-1» - возобновление действия;
- SomeComment - текстовое значение комментария владельца сертификата ключа подписи.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Удостоверяющего центра принимает по нему решение.

В случае отказа в возобновлении действия сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра возобновляет действие сертификата ключа подписи.

10.6.2. Возобновление действия сертификата ключа подписи Пользователя УЦ на основании заявления в бумажной форме

Заявление в бумажной форме предоставляется в Удостоверяющий центр по форме Приложения №9 к настоящему Регламенту посредством почтовой либо курьерской связи.

После предоставления заявления ответственное лицо Удостоверяющего центра принимает решение о возобновлении действия сертификата ключа подписи.

В случае отказа в возобновлении действия сертификата ключа подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник Удостоверяющего центра возобновляет действие сертификата ключа подписи.

10.7. Получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром

Получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром осуществляется на основании заявления Пользователя Удостоверяющего центра. Данное заявление оформляется по форме Приложения №10 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

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

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа подписи, которая предоставляется Пользователю Удостоверяющего центра.

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

10.8. Подтверждение подлинности ЭЦП в электронном документе

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

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

В данном случае для подтверждения подлинности ЭЦП в электронных документах Пользователь Удостоверяющего центра подает заявление в Удостоверяющий центр по форме, приведенной в Приложении № 11.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭЦП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭЦП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭЦП.

Обязательным приложением к заявлению на подтверждение подлинности ЭЦП в электронном документе является магнитный носитель, содержащий:

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

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

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

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭЦП 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 ЭЦП в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет десять рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат электронного документа с ЭЦП не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по подтверждению подлинности ЭЦП осуществляется в рамках заключения отдельного договора (соглашения) между Удостоверяющим центром и Стороной, присоединившейся к Регламенту. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором (соглашением).

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

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов 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 подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной цифровой подписью с использованием сертификата ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов). OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭЦП Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;
- Сертификат ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности ЭЦП OCSP-ответа действителен;
- Закрытый ключ подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- Сертификат ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении Extended Key Usage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);
- Сертификат ключа подписи, статус которого установлен с использованием данного OCSP-ответа, издан Удостоверяющим центром и содержит в расширении Extended Key Usage или Application Policy область использования - Пользователь службы актуальных статусов (1.2.643.2.2.34.26).

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – <http://ocsp.cryptopro.ru/ocsp/ocsp.srf>. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых Удостоверяющим центром сертификатов ключей подписей.

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

- Подтверждена подлинность ЭЦП Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- Сертификат ключа подписи Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭЦП штампа времени действителен;
- Закрытый ключ подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;
- Сертификат ключа подписи Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);

- Сертификат ключа подписи, на котором сформирована ЭЦП электронного документа и к которому относится данный штамп времени, издан Удостоверяющим центром и содержит в расширении Extended Key Usage или Application Policy область использования - Пользователь службы штампов времени (1.2.643.2.2.34.25).

Адрес обращения к Службе штампов времени Удостоверяющего центра – <http://tsp.cryptopro.ru/tsp/tsp.srf>.

10.10. Прочие условия

10.10.1. Период времени действия закрытого ключа, соответствующего выданному сертификату ключа подписи Пользователя Удостоверяющего центра должен находиться в пределах периода времени, на который Стороной, присоединившейся к Регламенту (для юридических лиц) выдана соответствующая доверенность на совершение действий, определенных положениями настоящего Регламента для Пользователя Удостоверяющего центра

10.10.2. Заявления на регистрацию пользователя, заявления на изготовление сертификатов ключей подписей, заявления на аннулирование (отзыв), приостановление и возобновление действия сертификатов ключей подписей, а также доверенности, оформляемые для совершения действий в рамках настоящего Регламента, копии сертификатов ключей подписей, подготавливаемые в бумажной форме, могут быть направлены в Удостоверяющий центр с помощью факсимильной связи по телефону (495) 780-48-20 или электронной связи на адрес cpca@cryptopro.ru или info@cryptopro.ru.

10.10.3. Стороны признают равную юридическую силу собственноручной подписи, выполненной на указанных в п. 10.9.2 документах, и факсимильной подписи.

11. Структура сертификатов ключей подписей и сроки действия ключевых документов

11.1. Структура сертификата ключа подписи уполномоченного лица Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) = ЦС Path Length Constraint (Ограничение на длину пути –ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата Уполномоченного лица Удостоверяющего центра

11.2. Структура сертификата ключа подписи Пользователя Удостоверяющего центра (клиентский сертификат ключа подписи)

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Application Policy	Политика применения	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора закрытого ключа уполномоченного лица Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280

11.3. Структура сертификата ключа подписи Пользователя Удостоверяющего центра (серверный сертификат ключа подписи)

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (not Before): дд.мм.гггг чч:мм:сс GMT Действителен по (not After): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = Псевдоним (как правило, DNS-имя сервера) OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре, включающий область использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Application Policy	Политика применения	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре, включающий область использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора закрытого ключа уполномоченного лица Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OSCP
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280

11.4. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки 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, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего Центра

11.5. Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи содержат объектные идентификаторы (OID), определяющие отношения, при осуществлении которых электронный документ, подписанный ЭЦП, будет иметь юридическое значение.

11.6. Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре и определяющих отношения, возникающие между Удостоверяющим центром и пользователями Удостоверяющего центра, приведен в Приложении № 13 настоящего Регламента.

11.7. Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре и определяющих отношения, возникающие между пользователями Удостоверяющего центра - участниками конкретных информационных систем, устанавливается регламентирующими документами данной конкретной информационной системы.

11.8. Сертификат ключа подписи пользователя Удостоверяющего центра (клиентский сертификат) в расширении Extended Key Usage или Application Policy

должен содержать, включая, но не ограничиваясь, следующие области использования:

- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4).

В сертификат ключа подписи пользователя Удостоверяющего центра в расширение Extended Key Usage или Application Policy может добавляться область использования «Участие в электронных торгах (1.2.643.2.2.46.7.1)», устанавливающая возможность использования данного сертификата ключа подписи и соответствующего ему закрытого ключа подписи в информационных системах проведения электронных торгов.

11.9. Сертификат ключа подписи пользователя Удостоверяющего центра (серверный сертификат) в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Проверка подлинности сервера (1.3.6.5.5.7.3.1).

11.10. Сертификат ключа подписи пользователя Удостоверяющего центра с поддержкой сервисов Службы актуальных статусов сертификатов и Службы штампов времени в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4);
- Пользователь службы актуальных статусов (1.2.643.2.2.34.26);
- Пользователь службы штампов времени (1.2.643.2.2.34.25).

11.11. Сертификат ключа подписи, изготавливаемый Удостоверяющим центром для работы в системе «Портал доверенных услуг «ФГУП НИИ «Восход» в расширении Extended Key Usage должен содержать следующие области использования:

- Доступ к услугам портала (1.2.643.2.25.1.3.1);
- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4).

11.12. Сертификат ключа подписи, изготавливаемый Удостоверяющим центром для работы в системе «Портал доверенных услуг «ФГУП НИИ «Восход» должен содержать расширение Subject Alternative Name. Значение поля id-ms-san-sc-logon-upn указанного расширения должно содержать UPN-имя пользователя в формате: «имя_пользователя_имя_УЦ@trustportal.ru» или «имя_пользователя@имя_УЦ.trustportal.ru», где: «имя_пользователя» - уникальное имя владельца сертификата в пределах домена, «имя_УЦ» - имя удостоверяющего центра, выпустившего сертификат ключа подписи, зарегистрированное за данным Удостоверяющим центром после аттестации в системе «Портал доверенных услуг «ФГУП НИИ «Восход»

11.13. Сроки действия ключевых документов

11.13.1. Сроки действия ключевых документов Уполномоченного лица Удостоверяющего центра

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

Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации закрытого ключа уполномоченного лица Удостоверяющего центра.

Срок действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

11.13.2. Сроки действия ключевых документов Пользователей Удостоверяющего центра

Срок действия закрытого ключа Пользователя Удостоверяющего составляет 1 (Один) год.

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

Срок действия сертификата ключа подписи Пользователя Удостоверяющего центра (клиентский сертификат ключа подписи) не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

Срок действия сертификата ключа подписи Пользователя Удостоверяющего центра (серверный сертификат ключа подписи) составляет 1 (Один) год.

12. Дополнительные положения

12.1. Плановая смена ключей уполномоченного лица Удостоверяющего центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица Удостоверяющего центра выполняется не ранее, чем через 1 год и не позднее, чем через 1 год 3 месяца после начала действия закрытого ключа уполномоченного лица Удостоверяющего центра

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

- Уполномоченное лицо Удостоверяющего центра генерирует новый закрытый и соответствующий ему открытый ключ;

- Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

Уведомление пользователей о проведении смены ключей уполномоченного лица Удостоверяющего центра осуществляется посредством электронной почты.

Старый закрытый ключ уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого закрытого ключа уполномоченного лица Удостоверяющего центра.

12.2. Компрометация ключевых документов уполномоченного лица Удостоверяющего центра, внеплановая смена ключей уполномоченного лица Удостоверяющего центра

В случае компрометации закрытого ключа уполномоченного лица Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра аннулируется (отзывается). Все сертификаты, подписанные с использованием скомпрометированного ключа уполномоченного лица Удостоверяющего центра, считаются аннулированными.

Уведомление Пользователей УЦ о компрометации закрытого ключа уполномоченного лица Удостоверяющего центра осуществляется посредством размещения данной информации на сайте Удостоверяющего центра <http://cpca.cryptopro.ru> и рассылки соответствующего сообщения по электронной почте.

После аннулирования сертификата уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра (пункт 12.1 настоящего Регламента).

Все подписанные с использованием скомпрометированного закрытого ключа уполномоченного лица Удостоверяющего центра и действовавшие на момент компрометации закрытого ключа уполномоченного лица Удостоверяющего центра сертификаты ключей подписей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

12.3. Компрометация ключевых документов Пользователя Удостоверяющего центра

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

В случае компрометации или угрозы компрометации закрытого ключа Пользователь связывается с Удостоверяющим центром по телефону и приостанавливает действие сертификата, соответствующего скомпрометированному ключу, посредством подачи заявления на приостановление действия сертификата в устной форме (пункт 10.5.1 настоящего Регламента).

Если в течение срока приостановления действия сертификата ключа подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр автоматически аннулирует (отзовет) данный сертификат.

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 10.3 настоящего Регламента.

12.4. Конфиденциальность информации

12.4.1. Типы конфиденциальной информации

12.4.1.1. Закрытый ключ, соответствующий сертификату ключа подписи является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра

12.4.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи, считается конфиденциальной

12.4.2. Типы информации, не являющейся конфиденциальной

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

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

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

12.4.2.4. Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным

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

12.4.3. Исключительные полномочия Удостоверяющего центра

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

12.5. Хранение сертификатов ключей подписей в Удостоверяющем центре

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

12.6. Прекращение оказания услуг Удостоверяющим центром

12.6.1. В случае расторжения Регламента одной из Сторон все сертификаты ключей подписей, владельцами которых являются Пользователь УЦ - Сторона Регламента (если Сторона Регламента – физическое лицо) и Пользователи УЦ – полномочные представители Стороны Регламента (если Сторона Регламента – юридическое лицо), аннулируются (отзываются) Удостоверяющим центром

12.7. Форс-мажор

12.7.1. 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

12.7.2. 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

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

12.7.4. 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

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

12.7.6. 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

13. Список приложений

13.1. Приложение №1. Форма заявления о присоединении к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания)

13.2. Приложение №2. Форма заявления на регистрацию Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО»

13.3. Приложение №3. Форма доверенности Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» на осуществление действий в рамках Регламента Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания)

13.4. Приложение №4. Форма заявления на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» (при изготовлении сертификата посредством web-интерфейса)

13.5. Приложение №5. Форма заявления на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» (при изготовлении сертификата на основе файла запроса)

13.6. Приложение №6. Форма заявления на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

13.7. Приложение №7. Форма заявления на отзыв доверенности на осуществление действий в рамках Регламента Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания)

13.8. Приложение №8. Форма заявления на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

13.9. Приложение №9. Форма заявления на возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

13.10. Приложение №10. Форма заявления на получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром ООО «КРИПТО-ПРО»

13.11. Приложение №11. Форма заявления на подтверждение подлинности электронной цифровой подписи в электронном документе

13.12. Приложение №12. Форма печати сертификата ключа подписи на бумажном носителе, издаваемого Удостоверяющим центром ООО «КРИПТО-ПРО»

13.13. Приложение №13. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «КРИПТО-ПРО», определяющих отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение

Приложение №1
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления о присоединении к Регламенту)

Для юридических лиц

Заявление о присоединении к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО» (Распределенная схема обслуживания)*

(наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) условия которого определены ООО «КРИПТО-ПРО» и опубликованы на сайте Удостоверяющего центра ООО «КРИПТО-ПРО» по адресу <http://cpca.cryptopro.ru/reglament/reglamentdist.pdf>.

С Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от «_____» _____ 20__ г.

Уполномоченное лицо

Удостоверяющего центра

ООО «КРИПТО-ПРО» _____

Печать Удостоверяющего центра

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

Приложение №1
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления о присоединении к Регламенту)

Для физических лиц

Заявление о присоединении к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО» (Распределенная схема обслуживания)*

Я, _____
(фамилия, имя, отчество)

(серия и номер паспорта)

кем и когда выдан)

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) условия которого определены ООО «КРИПТО-ПРО» и опубликованы на сайте Удостоверяющего центра ООО «КРИПТО-ПРО» по адресу <http://cpca.cryptopro.ru/reglament/reglamentdist.pdf>.

С Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Фамилия И.О.

Подпись и Дата подписания заявления

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО» (Распределенная схема обслуживания) зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от « _____ » _____ 20__ г.

Уполномоченное лицо
Удостоверяющего центра
ООО «КРИПТО-ПРО» _____

Печать Удостоверяющего центра

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

Приложение №2
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на регистрацию)

Для юридических лиц

**Заявление на регистрацию Пользователя
в Удостоверяющем центре ООО «КРИПТО-ПРО»**

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

в лице _____,
(должность)

(фамилия, имя, отчество)

действующего на основании _____

Просит зарегистрировать уполномоченного представителя

(фамилия, имя, отчество)

в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО», наделить полномочиями Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», установленными Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО» в соответствии с указанными в настоящем заявлении идентификационными данными:

Title (T)	Должность
CommonName (CN) ¹	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	RU
E-Mail (E)	Адрес электронной почты

Настоящим _____
(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных Удостоверяющим центром ООО «КРИПТО-ПРО» и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

¹ - Обязательным для заполнения полем является Common Name (CN). Необходимость установления значений остальных полей определяется заявителем

Приложение №2
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на регистрацию)

Для физических лиц

Заявление на регистрацию Пользователя
в Удостоверяющем центре ООО «КРИПТО-ПРО»

Я, _____
(фамилия, имя, отчество)

_____ (серия и номер паспорта)

_____ кем и когда выдан)

прошу зарегистрировать меня в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО», наделить полномочиями Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», установленными Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО» в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN) ¹	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	RU
E-Mail (E)	Адрес электронной почты

Настоящим _____
(фамилия, имя, отчество)

соглашается с обработкой своих персональных данных Удостоверяющим центром ООО «КРИПТО-ПРО» и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

«____» _____ 20____ г.

¹ - Обязательным для заполнения полем является Common Name (CN). Необходимость установления значений остальных полей определяется заявителем

Приложение №3
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма доверенности Пользователя Удостоверяющего центра)

Доверенность

г. _____ «_____» _____ 20__ г.

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____ (фамилия, имя, отчество)

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

выступать в роли Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» и осуществлять действия в рамках Регламента Удостоверяющего центра ООО «КРИПТО-ПРО», установленные для Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

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

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

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

подтверждаю.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №4
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на изготовление сертификата
при его изготовлении посредством web-интерфейса)

Для юридических и физических лиц

**Удостоверяющий Центр ООО «КРИПТО-ПРО»
Заявление на изготовление сертификата открытого ключа**

Прошу изготовить сертификат открытого ключа в соответствии с указанными данными:

Сведения о запросе на сертификат:

Этот запрос:

Кем выпущен:

User1

Версия: 1 (0x0)

Субъект запроса на сертификат: CN = User1

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-94

Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C
7DF9 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180
7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1
561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9

Атрибуты запроса на сертификат X.509

1. Атрибут 1.3.6.1.4.1.311.13.2.3

Название: Версия ОС

Значение: 5.0.2195.2

2. Атрибут 1.3.6.1.4.1.311.2.1.14

Название: Расширения сертификатов

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)

2. Расширение 1.2.840.113549.1.9.15

Название: Возможности SMIME

Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21

3. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Пользователь Центра Регистрации(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

Защищенная электронная почта(1.3.6.1.5.5.7.3.4)

3. Атрибут 1.3.6.1.4.1.311.13.2.2

Название: CSP заявки

Сведения о провайдере

Назначение ключа : ОБМЕН

Название провайдера : Crypto-Pro GOST R 34.10-94 Cryptographic Service Provider

Подпись провайдера : AA03 C083 A1B5 CCDC 20A0 F6A9 29D0 F124 8374 2251 6F71 C51A 52D5 469B 684B
7B7D 342F E0D8 8DDB 09EB B3BF 8DA6 3C98 AF07 327E 7EEB A121 A372 CA57 030A 87D2 AFA9 CDBB
D3AA 7575 AA85 01B7 0AB3 79B5 98BA 8453 9B62 AA33 AA4C F07E 6043 64AB BCA5 0A4B EB59 A3D0 E55B
D306 78A8 0B0B B05E 79F0 9001 E7B1 E133 B708 C11D 6AA1 4423 0000 0000 0000 0000

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-94

Параметры: 0500

Значение: BABC 1455 ADA3 DC7F 0EC9 3A1A 5020 CODE F561 C757 2986 BB2E B180 A5B0 091A 7F0A 6FA1
1A6E EE48 A366 B904 7288 A311 D966 BB2F FC7C EB75 3F0A 49ED A651 3E10 258A

Подпись владельца закрытого ключа: _____ /
" ____ " _____ 20__ г.

Подпись руководителя организации (для юридических лиц): _____ /
" ____ " _____ 20__ г.
М.П.

Приложение №5
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на изготовление сертификата
при его изготовлении на основе файла запроса)

Для юридических лиц

Заявление на изготовление сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

Просит изготовить сертификат ключа подписи уполномоченного представителя

(фамилия, имя, отчество)

на основании предоставленного файла запроса на сертификат ключа подписи в соответствии с указанными в настоящем заявлении данными:

Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	RU
E-Mail (E)	Адрес электронной почты

Приложение №5
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на изготовление сертификата
при его изготовлении на основе файла запроса)
(продолжение)

Текст запроса на сертификат ключа подписи формата PKCS#10 в кодировке Base64:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC4jCCAo8CAQAwYAxITAfBgkqhkiG9w0BCQEWEm12YW5vdkBtLXJlZXN0ci5y
dTElMAkGA1UEBhMCU1UxDzANBgNVBACTBk1vc2NvdzEVMBMGA1UEChMMT3JnYW5p
emF0aw9uMQ0wCwYDVQQLLEwREZXB0MRcwFQYDVQQDEw5JdmFuIEkuIE12YW5vdjBj
MBwGBiqFAwICEzASBgqhQMCAiQABgcqhQMCAh4BA0MABEBog51WRaScCe7qMJ3g
2s+zr08y4G5VhcaIdxWIYKwmcHL8AHKGC2pm0WCmE/XzUZorhycAYrUaH0gstA9C
nz17oIIBoDAABgorBgEEAYI3DQIDMQwwCjUuMC4yMTk1LjIwYwYKKwYBBAGCNwIB
DjFVMFMwDgYDVROPAQH/BAQDAgTwMBkGCSqGSIb3DQEJDwQMMaowCAYGKoUDAgIV
MCYGA1UdJQQfMB0GCCsGAQUFBwMCBggrBgEFBQcDBAYHKOUDAgIiBjCCARsGCisG
AQQBgjcNAgIxggELMIIBBwIBAR52AEMAcgB5AHAAdABvAC0AUABYAG8AIAABAE8A
UwBUACAAUgAgADMANAAuADEAMAAtADIAMAAdAEIAIDAHIAeQBwAHQAbwBnAHIA
YQBwAGgAaQBJACAAUwBIAHIAAdgBpAGMAZQAgAFAAcgBvAHYAaQBkAGUAcgOBiQAK
ofCLPzGSbmXMEex/cq9WymQT+3kQ1CRX0bRn0sM1GVV4AxJLfMS5x1PX/wwKxIv9
vnjdFdnXck1LJ5cw8g9kkmzdNEcEMgPYEi0xttZ9r3aTsIEjBEn7+1h8IgY+yDy
deR9DgPvC/QFS0diXCWYESkt2PiiAyAY/4WmVS1NSwAAAAAAAAAAMAoGBiqFAwIC
AwUAA0EAixD6RSeDYbF/VVjPfi+H+klhKaz5MbFNRA9BVIViFS3ccRvNZVpEfUFx
HriR0kQqa3/9hfEWRAupRwMye/3CMg==
-----END NEW CERTIFICATE REQUEST-----
```

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №5
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на изготовление сертификата
при его изготовлении на основе файла запроса)

Для физических лиц

Заявление на изготовление сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

Я, _____
(фамилия, имя, отчество)

(серия и номер паспорта)

кем и когда выдан)

прошу изготовить сертификат ключа подписи на основании предоставленного файла запроса на сертификат ключа подписи в соответствии с указанными в настоящем заявлении данными:

CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	RU
E-Mail (E)	Адрес электронной почты

Приложение №5
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на изготовление сертификата
при его изготовлении на основе файла запроса)
(продолжение)

Текст запроса на сертификат ключа подписи формата PKCS#10 в кодировке Base64:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC4jCCAo8CAQAwYAxITAFBgkqhkiG9w0BCQEWEm12YW5vdkBtLXJlZXN0ci5y
dTElMAkGA1UEBhMCU1UxDzANBgNVBACTBk1vc2NvdzEVMBMGA1UEChMMT3JnYW5p
emF0aw9uMQ0wCwYDVQQLEwREZXB0MRcwFQYDVQQDEw5JdmFuIEkuIE12YW5vdjBj
MBwGBiqFAwICEzASBgqhQMCAiQABgcqhQMCAh4BA0MABEBog51WRaScCe7qMJ3g
2s+zr08y4G5VhcaIdxWIYKwmcHL8AHKGC2pm0WCmE/XzUZorhycAYrUaH0gstA9C
nz17oIIBoDAABgorBgEEAYI3DQIDMQwwCjUuMC4yMTk1LjIwYwYKKwYBBAGCNwIB
DjFVMFMwDgYDVROPAQH/BAQDAgTwMBkGCSqGSIb3DQEJDDwQMMAowCAYGKoUDAgIV
MCYGA1UdJQQfMB0GCCsGAQUFBwMCBggrBgEFBQcDBAYHKOUDAgIiBjCCARsGCisG
AQQBgjcNAgIxggELMIIBBwIBAR52AEMAcgB5AHAAdABvAC0AUABYAG8AIAABAE8A
UwBUACAAUgAgADMANAAuADEAMAAtADIAMAAwADEAIABDARIAeQBwAHQAbwBnAHIA
YQBwAGgAaQBjACAAUwBIAHIAAdgBpAGMAZQAgAFAAcgBvAHYAaQBkAGUAcg0BiQAK
ofCLPzGSbmXMEex/cq9WymQT+3kQ1CRX0bRn0sMlGVV4AxJLfMS5x1PX/wwKxIv9
vnjdFdnXck1LJ5cw8g9kkpMzdNEcEMgPYEi0xttZ9r3aTsIEjBEn7+1h8IgY+yDy
deR9DgPvC/QFS0diXCWYESkt2PiiAyAY/4WmVS1NSwAAAAAAAAAAMAOGBiqFAwIC
AwUAA0EAixD6RSeDYbF/VVjPfi+H+klhKaz5MbFNra9BVIViFS3ccRvNZVpEfUFx
HriR0kQqa3/9hfEWRAupRwMye/3CMg==
-----END NEW CERTIFICATE REQUEST-----
```

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Приложение №6
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на аннулирование (отзыв) сертификата)

Для юридических лиц

Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

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

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина отзыва сертификата)

Просит аннулировать (отозвать) сертификат ключа подписи своего
уполномоченного представителя – Пользователя Удостоверяющего центра ООО
«КРИПТО-ПРО»: _____
(фамилия, имя, отчество)

содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №6
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на аннулирование (отзыв) сертификата)

Для физических лиц

Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

Я, _____
(фамилия, имя, отчество)

в связи с _____
(причина отзыва сертификата)

прошу аннулировать (отозвать) сертификат ключа подписи, содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Приложение №7

к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на отзыв доверенности Пользователя Удостоверяющего центра)

Заявление на отзыв доверенности

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

Заявляет, что отзывает Доверенность № _____ от «_____» _____ 20__ года,
выданную для представления в Удостоверяющий центр ООО «КРИПТО-ПРО»

своему полномочному представителю _____

(фамилия, имя, отчество)

и просит аннулировать (отозвать) все действующие сертификаты ключей подписей и
сертификаты ключей подписей, действие которых приостановлено, владельцем
которых является

(фамилия, имя, отчество)

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №8
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на приостановление действия сертификата)

Для юридических лиц

Заявление на приостановление действия сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

(полное наименование организации, включая организационно-правовую форму)

В лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие сертификата ключа подписи своего
уполномоченного представителя – Пользователя Удостоверяющего центра ООО
«КРИПТО-ПРО»:

(фамилия, имя, отчество)

содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Срок приостановления действия сертификата _____ дней.

(количество дней прописью)

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №8
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на приостановление действия сертификата)

Для физических лиц

Заявление на приостановление действия сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

Я, _____
(фамилия, имя, отчество)

прошу приостановить действие сертификата ключа подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

«____» _____ 20____ г.

Приложение №9
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на возобновление действия сертификата)

Для юридических лиц

Заявление на возобновление действия сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»:

(фамилия, имя, отчество)

содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №9
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на возобновление действия сертификата)

Для физических лиц

Заявление на возобновление действия сертификата ключа подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

Я, _____
(фамилия, имя, отчество)

прошу возобновить действие сертификата ключа подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

« ____ » _____ 20 ____ г.

Приложение №10
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на получение информации о статусе сертификата)

Для юридических лиц

Заявление на получение информации о статусе сертификата ключа подписи,
изданного Удостоверяющим центром ООО «КРИПТО-ПРО»

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

В лице _____,
(должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____

Просит предоставить информацию о статусе следующего сертификата ключа подписи:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Время¹ (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

¹ _____
Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №10
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на получение информации о статусе сертификата)

Для физических лиц

Заявление на получение информации о статусе сертификата ключа подписи,
изданного Удостоверяющим центром ООО «КРИПТО-ПРО»

Я, _____
(фамилия, имя, отчество)

Прошу предоставить информацию о статусе следующего сертификата ключа подписи:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Время¹ (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

_____/_____
«_____» _____ 20____ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №11
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на подтверждение подлинности ЭЦП)

Для юридических лиц

Заявление на подтверждение подлинности электронной цифровой подписи в
электронном документе

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подтвердить подлинность ЭЦП в электронном документе на основании
следующих данных:

1. Файл формата CMS, содержащий сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭЦП в электронном документе на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX;
 2. Файл, содержащий подписанные ЭЦП данные и значение ЭЦП формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение ЭЦП формата CMS, на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX
 3. Время¹ на момент наступления которых требуется подтвердить подлинность ЭЦП: « ____ : ____ » « ____ / ____ / ____ »;
- Час минута день месяц год

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

¹ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то подтверждение подлинности ЭЦП устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №11
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма заявления на подтверждение подлинности ЭЦП)

Для физических лиц

Заявление на подтверждение подлинности электронной цифровой подписи в
электронном документе

Я, _____
(фамилия, имя, отчество)

прошу подтвердить подлинность ЭЦП в электронном документе на основании
следующих данных:

1. Файл формата CMS, содержащий сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭЦП в электронном документе на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX;
2. Файл, содержащий подписанные ЭЦП данные и значение ЭЦП формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение ЭЦП формата CMS, на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX
3. Время¹ на момент наступления которых требуется подтвердить подлинность ЭЦП: « ____ : ____ » « ____ / ____ / ____ »;

Час
минута
день
месяц
год

Пользователь Удостоверяющего центра
ООО «КРИПТО-ПРО»

_____/_____
« ____ » _____ 20 ____ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то подтверждение подлинности ЭЦП устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №12
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)
(Форма сертификата ключа подписи на бумажном носителе)

Удостоверяющий центр ООО «КРИПТО-ПРО»
Сертификата ключа подписи

Сведения о сертификате:**Кому выдан:**

Фамилия Имя Отчество

Кем выдан:

УЦ КРИПТО-ПРО

Версия: 3 (0x2)**Серийный номер:** 14F5 9CF2 0000 0000 003A**Издатель сертификата:** CN = УЦ КРИПТО-ПРО, O = ООО КРИПТО-ПРО, L = Москва, C = RU, E = cpca@cryptopro.ru**Срок действия:**

Действителен с: 15 октября 2003 г. 12:03:00 UTC

Действителен по: 15 октября 2004 г. 12:12:00 UTC

Владелец сертификата: CN = Фамилия Имя Отчество**Открытый ключ:**

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-94

Идентификатор: 1.2.643.2.2.20

Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9
 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E
 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4
 C23F E5EA ECD9 E6B5 A9

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных(F0)

2. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Защищенная электронная почта(1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации(1.2.643.2.2.34.6)

Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: 56BD CA83 3029 0673 CA83 3381 16D4 AF10 C3D6 9A75

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа= d1 27 44 30 15 0a de 17 fa f9 e1 9f 3f c7 1a 0d c8 45 a7 9f

5. Расширение 2.5.29.31

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распространения списка отзыва (CRL) Имя точки распространения: Полное имя:

URL=http://cdp.cryptopro.ru/RA/CDP/d1274430150ade17faf9e19f3fc71a0dc845a79f.crl

URL=http://cpca.cryptopro.ru/RA/CDP/d1274430150ade17faf9e19f3fc71a0dc845a79f.crl

6. Расширение 1.3.6.1.5.5.7.1.1

Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния

сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.cryptopro.ru/ocsp/ocsp.srf

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2001

Идентификатор: 1.2.643.2.2.3

Параметры: 0500

Значение: 826C DDFB 331C 58C5 FD3D 9233 4A1D 2D7A B973 387C 8E8A DD3D 6FCE 0573 508A 3DC4 B29F 5961 FB6C

D1EB 1B40 37C7 8473 5B0F FECA 5E38 EA0C 3890 C77A C97E BD18 873A

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

Подпись Уполномоченного лица УЦ: _____/_____

«___» _____ 20__ г.

М.П.

Приложение №13
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
(Распределенная схема обслуживания)

Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «КРИПТО-ПРО» и, определяющих отношения, возникающие между Удостоверяющим центром ООО «КРИПТО-ПРО» и пользователями Удостоверяющего центра ООО «КРИПТО-ПРО», при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение

	OID	Область применения
1.	1.2.643.2.2.34.6	Пользователь Центра Регистрации – формирование электронной цифровой подписи электронных документов, определенных Регламентом для Пользователя Удостоверяющего центра
2.	1.3.6.1.5.5.7.3.9	Подпись ответа службы OCSP – формирование электронной цифровой подписи ответов Службы актуальных статусов сертификатов
3.	1.3.6.1.5.5.7.3.8	Установка штампа времени – формирование электронной цифровой подписи штампов времени, предоставляемых Службой штампов времени