Утвержден
Приказом ООО «КРИПТО-ПРО»
от «01» июня 2013 г. № 2

РЕГЛАМЕНТ

Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Схема обслуживания: распределенная с оператором)

Редакция № 4

г. Москва
2013

1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дельнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва Государственным учреждением Московской регистрационной палатой (Свидетельство о регистрации № 001.602.749 выдано 16.11.1999г.); 29.01.2003г. внесена запись о юридическом лице, зарегистрированном до 01.07.2001г. за основным государственным регистрационным номером 1037700085444.

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 по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 8713Р от 22 апреля 2010 г. на право осуществления** распространения шифровальных (криптографических) средств;

2. **Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 8712Х от 22 апреля 2010 г. на право осуществления** технического обслуживания шифровальных (криптографических) средств;

3. **Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 8714У от 22 апреля 2010 г. на право** предоставления услуг в области шифрования информации;

Реквизиты ООО «КРИПТО-ПРО»:
Полное наименование: Общество с ограниченной ответственностью «КРИПТО-ПРО»
Юридический адрес: 105318, г. Москва, ул. Ибрагимова, д. 31, офис 30Б
Адрес нахождения Удостоверяющего центра: 127018, г. Москва, ул. Сущевский вал, д. 18
Адрес для корреспонденции: 127018, г. Москва, А/Я «КРИПТО-ПРО»
Банковские реквизиты (наименование банка, БИК, р/с, к/с):

- ОАО Сбербанк России, г. Москва
- БИК 044525225
- Р/с 40702810638040112712
- К/с 30101810400000000225

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) 995-48-20; e-mail: cpca@cryptopro.ru, info@cryptopro.ru

2. Термины и определения

Автоматизированное рабочее место администратора Центра регистрации (АРМ администратора ЦР) – специализированное программное обеспечение, предоставляемое Оператору Удостоверяющего центра для регистрации пользователей, принятия решений по изготовлению и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра.

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписей Операторов и Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром расписываться собственноручной подписью в копиях сертификатов ключей подписей на бумажном носителе, изданных Удостоверяющим центром (заверять копии сертификатов ключей подписей).

Веб-интерфейс, предоставляемый Удостоверяющим центром – интерфейс взаимодействия Удостоверяющего центра с Пользователем и Оператором Удостоверяющего центра, предназначенный для управления сертификатами ключей подписей, реализованный в виде набора веб-страниц и размещенный на веб-узле Удостоверяющего центра.

Владелец сертификата ключа подписи – 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).

Закрытый ключ электронной цифровой подписи (закрытый ключ подписи) – ключ электронной подписи, являющийся уникальной последовательностью символов, известной владельцу сертификата ключа подписи и предназначенной 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.

Информационная система Уполномоченной Организации - обобщенное понятие корпоративной информационной системы Уполномоченной Организации, в которой используются закрытые ключи и сертификаты ключей подписей, и предоставляющей определенные услуги участникам этой системы.

Копия сертификата ключа подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный Оператором Удостоверяющего центра и печатью Уполномоченной Организации, либо Администратором Удостоверяющего и печатью Удостоверяющего центра.

Маркер временного доступа - идентификатор (десятичное число) и секретный пароль (пятизначное символьное значение), предоставляющийся Пользователю и Оператору Удостоверяющего центра, не имеющим действующего закрытого ключа, для формирования и передачи в Удостоверяющий центр запроса на сертификат ключа подписи посредством веб-интерфейса, предоставляемого Удостоверяющим центром.

Оператор предоставления услуг Удостоверяющего Центра, Уполномоченная Организация – юридическое лицо, заключившее с Удостоверяющим центром договор на предоставление услуг по изготовлению сертификатов ключей подписей и уполномоченное Удостоверяющим центром осуществлять регистрацию пользователей, изготовление и управление сертификатами ключей подписей Пользователей Удостоверяющего центра.

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.

Оператор Удостоверяющего центра – физическое лицо, являющееся сотрудником Уполномоченной Организации, наделенное Удостоверяющим центром и Уполномоченной Организацией правами по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра и уполномоченное Удостоверяющим центром расписываться собственноручной подписью на копиях сертификатов ключей подписей Пользователей Удостоверяющего центра (заверять копии сертификатов ключей подписей).

Открытый ключ электронной цифровой подписи (открытый ключ подписи) – ключ проверки электронной подписи, являющийся уникальной последовательностью символов, соответствующий закрытому ключу электронной цифровой подписи, предназначенной для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Пользователь Удостоверяющего центра – физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся участником Информационной системы Уполномоченной Организации.

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

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 на регистрацию пользователей 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 (сертификат ключа электронной цифровой подписи, сертификат открытого ключа) – неквалифицированный сертификат ключа проверки электронной подписи, являющийся электронным документом с электронной цифровой подписью уполномоченного лица 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.

Служба актуальных статусов сертификатов – сервис Удостоверяющего центра, обеспечивающий информирование пользователей о статусе сертификатов ключей подписей по протоколу OCSP (Online Certificate Status Protocol).

Служба штампов времени – сервис Удостоверяющего центра, обеспечивающий предоставление Пользователям Удостоверяющего центра штампов времени по протоколу TSP (Time-Stamp Protocol).

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны 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, средство электронной подписи) «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 по изготовлению и управлению неквалифицированными сертификатами ключей проверки электронной подписи в соответствии с Федеральным законом «Об электронной подписи» в целях обеспечения применения участниками Информационной Системы неквалифицированной усиленной электронной подписи.

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) – усиленная неквалифицированная электронная подпись, являющаяся реквизитом электронного документа, предназначенным для защиты данного электронного документа от подделки, полученная 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 криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

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

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

3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент Удостоверяющего центра ООО «КРИПТО-ПРО» (Схема обслуживания: распределенная с оператором), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

3.1.2. Сторонами Регламента (далее Стороны) являются Удостоверяющий центр - ООО «КРИПТО-ПРО» и Оператор предоставления услуг Удостоверяющего центра (Уполномоченная Организация).

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

3.2. Применение Регламента

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

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

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

3.3. Изменение (дополнение) Регламента

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

3.3.2. 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/reglamentoper.pdf.

3.3.3. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении одного месяца со дня размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра.

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

3.3.5. 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.

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

4. Предоставление информации

4.1. Удостоверяющий центр предоставляет Стороне, присоединившейся к Регламенту по ее требованию:

4.1.1. Копию лицензии ФСБ России на осуществление профессиональной деятельности по распространению шифровальных (криптографических средств).

4.1.2. Копию лицензии ФСБ России на осуществление профессиональной деятельности по техническому обслуживанию шифровальных (криптографических средств).

4.1.3. Копию лицензии ФСБ России на осуществление профессиональной деятельности на предоставление услуг в области шифрования информации.

4.1.4. Копию лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

4.2. Удостоверяющий центр вправе запросить у Оператора предоставления услуг Удостоверяющего центра, а Оператор предоставления услуг Удостоверяющего центра обязан предоставить Удостоверяющему центру документы, подтверждающие следующую информацию:

4.2.1. Наименование Организации, основной государственный регистрационный номер, идентификационный номер налогоплательщика;

4.2.2. Место регистрации и адрес места жительства полномочного представителя Оператора предоставления услуг Удостоверяющего центра – Оператора Удостоверяющего центра, зарегистрированного в Удостоверяющем центре;

4.2.3. Сведения, необходимые для идентификации Оператора Удостоверяющего центра: фамилия, имя, отчество, номер паспорта, кем и когда выдан.

5. Права и обязанности сторон

5.1. Удостоверяющий центр обязан:

5.1.1. Предоставить Оператору Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра.

5.1.2. 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.

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

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

5.1.5. Организовать свою работу по UTC (всемирное координированное время) с учетом часового пояса города Москвы. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

5.1.6. Обеспечить регистрацию Оператора в Удостоверяющем центре по заявлению на регистрацию в Удостоверяющем центре в соответствии с порядком, определенным в настоящем Регламенте.

5.1.7. 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.

5.1.8. Изготовить сертификат ключа подписи Оператора Удостоверяющего центра по заявлению на изготовление сертификата в соответствии с порядком, определенным в настоящем Регламенте.

5.1.9. Обеспечить изготовление сертификата ключа подписи Пользователя Удостоверяющего центра, в соответствии с порядком, определенным в настоящем Регламенте и уведомить об этом владельца изготовленного сертификата ключа подписи.

5.1.10. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей подписей.

5.1.11. Обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей подписей.

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

5.1.13. Обеспечить аннулирование (отзыв), приостановление и возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра в соответствии с порядком, определенным в настоящем Регламенте.

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

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

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

5.1.17. 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 (Один) час.

5.1.18. Предоставить Оператору предоставления услуг Удостоверяющего Центра необходимые средства и права по осуществлению регистрации пользователей в Удостоверяющем центре, изготовлению и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра.

5.2. Оператор предоставления услуг Удостоверяющего Центра (Уполномоченная Организация) обязан:

5.2.1. Известить Удостоверяющий центр об изменениях в наименовании Организации, государственного регистрационного номера, идентификационного номера налогоплательщика и по требованию Удостоверяющего Центра предоставить документы, указанные в п.4.2 настоящего Регламента, в течение 5-ти рабочих дней с момента регистрации изменений.

5.2.2. Оператор Удостоверяющего Центра, являющийся полномочным представителем Уполномоченной Организации обязан:

5.2.2.1. Формировать открытые и закрытые ключи подписи только с использованием средства электронной цифровой подписи и программного обеспечения, предоставленного Удостоверяющим центром.

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

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

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

5.2.2.5. 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 сертификата ключа подписи).

5.2.2.6. Немедленно обратиться в Удостоверяющий центр, с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а так же в случае, если Оператору Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

5.2.2.7. 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 в Удостоверяющий центр по момент времени официального уведомления об аннулировании (отзыве) сертификата, либо об отказе в аннулировании (отзыве).

5.2.2.8. 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 в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

5.2.2.9. Не использовать личный закрытый ключ до предоставления в Удостоверяющий центр подписанного сертификата ключа подписи на бумажном носителе, соответствующего данному закрытому ключу.

5.3. Удостоверяющий центр имеет право:

5.3.1. Отказать в регистрации в Удостоверяющем центре уполномоченному представителю Оператора предоставления услуг Удостоверяющего центра, в случае ненадлежащего оформления необходимых регистрационных документов.

5.3.2. Отказать в изготовлении сертификата ключа подписи Оператора Удостоверяющего центра в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи.

5.3.3. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключа подписи Оператора Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв), приостановление и возобновление действия сертификата ключа подписи.

5.3.4. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключа подписи Оператора и Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего сертификату.

5.3.5. По согласованию с Оператором предоставления услуг Удостоверяющего центра приостановить действие сертификата ключа подписи Оператора и Пользователя Удостоверяющего центра с обязательным уведомлением владельца сертификата ключа подписи, действие которого приостановлено, и указанием обоснованных причин.

5.3.6. Отказать в изготовлении сертификата ключа подписи Оператора и Пользователя Удостоверяющего центра в случае, если использованное Оператором и Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа подписи средство криптографической защиты информации (средство электронной цифровой подписи) не поддерживается Удостоверяющим центром.

5.4. Оператор предоставления услуг Удостоверяющего центра имеет право:

5.4.1. Заверять печатью Организации копии изготовленных Удостоверяющим центром сертификатов ключей подписей Пользователей Удостоверяющего центра.

5.4.2. Оператор Удостоверяющего центра и Пользователь Удостоверяющего центра имеют право:

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

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

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

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

5.4.3. Пользователь Удостоверяющего центра имеет право:

5.4.3.1. Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на регистрацию в электронном виде.

5.4.3.2. Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий Центр заявления на аннулирование (отзыв) сертификата ключа подписи в электронном виде.

5.4.3.3. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами для передачи по линиям связи в Удостоверяющий Центр заявления на приостановление действия сертификата ключа подписи в электронном виде.

5.4.3.4. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами для передачи по линиям связи в Удостоверяющий Центр заявления на возобновление действия сертификата ключа подписи в электронном виде.

5.4.4. Оператор Удостоверяющего центра имеет право:

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

5.4.4.2. 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.

5.4.4.3. 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.

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

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

5.4.4.6. Регистрировать в Удостоверяющем центре участников Информационной системы Уполномоченной Организации и заносить регистрационную информацию в Реестр Удостоверяющего центра.

5.4.4.7. Принимать по заявлению на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра решение по изготовлению сертификата ключа подписи.

5.4.4.8. Являясь уполномоченным представителем Удостоверяющего центра, расписываться собственноручной подписью на копиях изготовленных сертификатов ключей подписей, решение по изготовлению которых было принято данным Оператором Удостоверяющего центра.

5.4.4.9. Аннулировать (отзывать) сертификат ключа подписи Пользователя Удостоверяющего центра в течение срока действия соответствующего данному сертификату закрытого ключа.

5.4.4.10. Приостанавливать действие сертификата ключа подписи Пользователя Удостоверяющего центра в течение срока действия соответствующего данному сертификату закрытого ключа.

5.4.4.11. Возобновлять действие сертификата ключа подписи Пользователя Удостоверяющего центра в течение срока действия соответствующего данному сертификату закрытого ключа и срока, на который действие сертификата было приостановлено.

6. Ответственность сторон

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

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

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

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

6.5. Вся ответственность по регистрации Пользователей Удостоверяющего центра, занесению данных в сертификаты ключей подписей, принятию решений по изготовлению и управлению сертификатами ключей подписей, формированию копий сертификатов ключей подписей Пользователей Удостоверяющего центра полностью возлагается на Оператора Удостоверяющего центра, являющегося полномочным лицом Оператора предоставления услуг Удостоверяющего Центра (Уполномоченной Организации).

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

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

7. Разрешение споров

7.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий Центр - ООО «КРИПТО-ПРО» и Оператор предоставления услуг Удостоверяющего Центра (Уполномоченная Организация).

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

7.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

7.4. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в Арбитражном суде г. Москвы.

8. Порядок предоставления и пользования услугами Удостоверяющего Центра

8.1. Регистрация Оператора Удостоверяющего центра

Регистрация Оператора Удостоверяющего центра осуществляется на основании заявления на регистрацию по форме Приложения № 2 настоящего Регламента. Предоставление документов может быть осуществлено при личном прибытии Оператора в Удостоверяющий центр (либо его полномочного представителя) по предварительному согласованию с Администратором Удостоверяющего Центра, либо посредством почтовой или курьерской связи.

Для регистрации в Удостоверяющем центре Оператор предоставляет следующий пакет документов включающий:

- Заявление на регистрацию Оператора Удостоверяющего центра;
- Доверенность, выданная на имя лица, регистрирующегося в Удостоверяющем центре, и уполномочивающая указанное лицо выступать в роли Оператора Удостоверяющего центра и совершать действия, определенные положениями настоящего Регламента для Оператора Удостоверяющего центра. Оформляется по форме Приложения № 3 настоящего Регламента.

После осуществления регистрации Удостоверяющий центр сообщает Оператору секретную ключевую фразу и предоставляет необходимое программное обеспечение и лицензии на право его пользования в составе:

- URL адреса доступа к дистрибутивам АРМ администратора Центра регистрации и средства электронной цифровой подписи;
- URL адреса подключения к Удостоверяющему центру для Оператора Удостоверяющего центра и для Пользователей Удостоверяющего центра);
- Файл сертификата ключа подписи Уполномоченного лица Удостоверяющего центра.

Регистрация Оператора Удостоверяющего центра должна быть осуществлена в течение рабочего дня предоставления заявительных документов.

После успешной регистрации Оператор Удостоверяющего центра должен обратиться в Удостоверяющий центр с заявлением на изготовление сертификата ключа подписи (пункт 8.2. настоящего Регламента).

8.2. Генерация ключей и формирование первого сертификата ключа подписи Оператора Удостоверяющего центра

Генерация ключей и формирование первого сертификата ключа подписи Оператора Удостоверяющего центра может быть осуществлена в двух режимах (по выбору Оператора Удостоверяющего центра):

1. Формирование сертификата ключа подписи Оператора Удостоверяющего центра с генерацией ключей в Удостоверяющем центре;

2. Формирование сертификата ключа подписи Оператора Удостоверяющего центра с генерацией ключей на рабочем месте Оператора (с использованием АРМ администратора ЦР либо посредством веб-интерфейса, предоставляемого Удостоверяющим центром).

8.2.1. Формирование сертификата ключа подписи Оператора Удостоверяющего центра с генерацией ключей в Удостоверяющем центре

Формирование сертификата ключа подписи Оператора Удостоверяющего центра с генерацией ключей в Удостоверяющем центре осуществляется при личном прибытии в Удостоверяющий центр Оператора (либо его полномочного представителя) по предварительному согласованию с Администратором Удостоверяющего центра, и производится в течение рабочего дня прибытия Оператора Удостоверяющего центра.

Оператор подает в Удостоверяющий центр заявление на изготовление сертификата ключа подписи по форме Приложения №5 и предоставляет носитель закрытого ключа, поддерживаемый средством электронной цифровой подписи и Удостоверяющим центром.

На основании предоставленного заявления Администратор Удостоверяющего центра осуществляет генерацию ключей подписей, запись закрытого ключа подписи на предоставленный носитель, изготовление сертификата ключа подписи, запись сертификата ключа подписи на предоставленный носитель и распечатывает по форме Приложения №14 две копии сертификата ключа подписи.

Копии сертификата ключа подписи Оператора на бумажном носителе визируются уполномоченным на это лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и предоставляются Оператору Удостоверяющего центра. Оператор (либо его полномочный представитель) подписывает собственноручной подписью копии сертификата ключа подписи и один экземпляр возвращает Администратору Удостоверяющего центра.

8.2.2. Формирование сертификата ключа подписи Оператора Удостоверяющего центра с генерацией ключей на рабочем месте Оператора (с использованием АРМ администратора ЦР)

После установки и настройки АРМ администратора ЦР в соответствии с предоставленной эксплуатационной документацией Оператор Удостоверяющего Центра осуществляет генерацию пары ключей (закрытого и открытого ключа подписи) и формирование запроса на сертификат ключа подписи в файл формата PKCS#10 в кодировке Base64.

Оператор подает в Удостоверяющий центр заявление на изготовление сертификата ключа подписи на бумажном носителе по форме Приложения №6, включающее текст запроса на сертификат, и направляет в Удостоверяющий центр по электронной почте сообщение, содержащее:

- Subject (Тема письма): «Запрос на изготовление сертификата ключа подписи Оператора УЦ»;
- Body (Тело письма): «Прошу изготовить сертификат ключа подписи Оператора УЦ по запросу на сертификат ключа подписи, содержащемуся в настоящем сообщении»;
- файл запроса на сертификат формата PKCS#10 в кодировке Base64 в виде вложения.

Предоставление заявления на изготовление сертификата ключа подписи Оператора на бумажном носителе осуществляется посредством почтовой или курьерской связи.

Администратор Удостоверяющего центра осуществляет сравнение содержимого полученного по электронной почте файла запроса на сертификат с текстом запроса на сертификат, содержащимся в заявлении на изготовление сертификата ключа подписи Оператора на бумажном носителе.

В случае идентичности предоставленных данных Администратор Удостоверяющего центра осуществляет сравнение идентификационных данных, указанных в запросе на сертификат с идентификационными данными, указанными в заявлении на изготовление сертификата. При совпадении идентификационной информации Администратор Удостоверяющего центра изготавливает сертификат ключа подписи Оператора и распечатывает по форме Приложения №14 две копии сертификата ключа подписи на бумажном носителе.

Две копии сертификата ключа подписи Оператора на бумажном носителе визируются уполномоченным на это лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Оператору Удостоверяющего центра.

Администратор Удостоверяющего центра уведомляет сообщением по электронной почте Оператора об изготовлении сертификата ключа подписи, а также в виде вложения этого сообщения направляет ему файл, содержащий изготовленный сертификат ключа подписи.

Изготовление сертификата ключа подписи и уведомление Оператора об изготовлении сертификата должны быть осуществлены не позднее 5-ти рабочих дней следующих за рабочим днем, в течение которого было принято заявление на изготовление сертификата. Заявление на изготовление сертификата ключа подписи Оператора считается принятым Удостоверяющим центром, если получено собственно заявление на изготовление сертификата ключа подписи Оператора и получено сообщение, направленное по электронной почте и содержащее файл запроса на сертификат.

После получения двух копий сертификата ключа подписи на бумажном носителе и уведомления об изготовлении сертификата, содержащего изготовленный сертификат, Оператор подписывает собственноручной подписью две копии сертификата ключа подписи и одну копию направляет посредством почтовой или курьерской связи в Удостоверяющий центр. С помощью предоставленного Удостоверяющим центром программного обеспечения Оператор производит установку сертификата на своем рабочем месте.

После подтверждения получения Удостоверяющим центром завизированной Оператором копии сертификата ключа подписи на бумажном носителе, Оператор приступает к выполнению возложенных на него обязанностей.

8.2.3. Формирование сертификата ключа подписи Оператора Удостоверяющего центра с генерацией ключей в Удостоверяющем центре посредством веб-интерфейса, предоставляемого Удостоверяющим центром

После успешной регистрации Оператор Удостоверяющего центра обращается к Администратору Удостоверяющего центра с просьбой предоставить маркер временного доступа для формирования запроса на изготовление сертификата ключа подписи.

После предоставления маркера временного доступа Оператор Удостоверяющего центра с использованием веб-интерфейса, предоставляемого Удостоверяющим центром, генерирует ключи и формирует запрос на сертификат ключа подписи. После успешного формирования запроса на сертификат ключа подписи Оператор распечатывает заявление на изготовление сертификата ключа подписи на бумажном носителе по форме Приложения № 7 и оформляет его.

Предоставление заявления на изготовление сертификата ключа подписи Оператора на бумажном носителе осуществляется посредством почтовой или курьерской связи.

Администратор Удостоверяющего центра осуществляет сравнение запроса на сертификат с содержимым заявления на изготовление сертификата на бумажном носителе.

В случае идентичности предоставленных данных Администратор Удостоверяющего центра изготавливает сертификат ключа подписи Оператора и распечатывает по форме Приложения №14 две копии сертификата ключа подписи на бумажном носителе.

Две копии сертификата ключа подписи Оператора на бумажном носителе визируются уполномоченным на это лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Оператору Удостоверяющего центра.

Администратор Удостоверяющего центра уведомляет сообщением по электронной почте Оператора об изготовлении сертификата ключа подписи. После получения указанного сообщения Оператор посредством веб-интерфейса Удостоверяющего центра производит установку изданного сертификата ключа подписи на своем рабочем месте.

Изготовление сертификата ключа подписи и уведомление Оператора об изготовлении сертификата должны быть осуществлены не позднее 5-ти рабочих дней следующих за рабочим днем, в течение которого было принято заявление на изготовление сертификата.

После получения двух копий сертификата ключа подписи на бумажном носителе, Оператор подписывает собственноручной подписью две копии сертификата ключа подписи и одну копию направляет посредством почтовой или курьерской связи в Удостоверяющий центр.

После подтверждения получения Удостоверяющим центром завизированной Оператором копии сертификата ключа подписи на бумажном носителе, Оператор приступает к выполнению возложенных на него обязанностей.

8.3. Плановая смена ключей Оператора Удостоверяющего центра

За 14 календарных дней до окончания срока действия закрытого ключа Удостоверяющий центр по электронной почте уведомляет Оператора о необходимости осуществления плановой смены ключей.

Удостоверяющий центр осуществляет изготовление нового сертификата ключа подписи Оператора по заявлению на изготовление сертификата не ранее 14-ти календарных дней и не позднее 5-ти календарных дней до окончания срока действия закрытого ключа Оператора Удостоверяющего Центра.

Заявления, поступившие в Удостоверяющий центр ранее или позднее установленного срока, рассмотрению не подлежат.

Оператор Удостоверяющего центра с помощью АРМ администратора ЦР осуществляет генерацию новой пары ключей (закрытого и открытого ключа подписи), формирование и предоставление в Удостоверяющий центр заявления на изготовление сертификата ключа подписи в электронном виде. Заявление на изготовление сертификата в электронном виде 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 Оператора Удостоверяющего центра.

Администратор Удостоверяющего Центра на основании поступившего заявления на изготовление сертификата ключа подписи изготавливает сертификат ключа подписи Оператора и распечатывает по форме Приложения №14 два экземпляра сертификата ключа подписи на бумажном носителе.

Два экземпляра сертификата ключа подписи Оператора на бумажном носителе визируются уполномоченным на это лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Оператору Удостоверяющего центра.

Изготовление сертификата ключа подписи осуществляется не позднее 5-ти рабочих дней следующих за рабочим днем, в течение которого было принято заявление на изготовление сертификата.

После получения двух экземпляров сертификата ключа подписи на бумажном носителе, Оператор подписывает их собственноручной подписью и один экземпляр направляет посредством почтовой или курьерской связи в Удостоверяющий центр.

После подтверждения получения Удостоверяющим центром завизированного Оператором сертификата ключа подписи на бумажном носителе, Оператор может использовать для выполнения возложенных на него обязанностей новый сертификат ключа подписи и соответствующий ему закрытый ключ.

8.4. Внеплановая смена ключей Оператора Удостоверяющего центра

Внеплановая смена ключей осуществляется Оператором Удостоверяющего центра в следующих случаях:

- При компрометации закрытого ключа Оператора Удостоверяющего центра;
- При компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра;
- В случае, если Оператор Удостоверяющего центра по каким-либо причинам не смог осуществить плановую смену ключей в установленные для этой процедуры сроки;

Генерация ключей и формирование сертификата ключа подписи Оператора Удостоверяющего центра осуществляется в соответствии с пунктом 8.2 настоящего Регламента.

8.5. Аннулирование (отзыв) сертификата ключа подписи Оператора Удостоверяющего центра

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

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

В случае прекращения действия настоящего Регламента, отзыва доверенности Оператора, истечения срока, на который действие сертификата ключа подписи было приостановлено, отзыва сертификата Оператора по его заявлению Удостоверяющий центр должен официально уведомить Оператора 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 Оператора Удостоверяющего центра по истечении срока его действия временем аннулирования сертификата ключа подписи Оператора Удостоверяющего центра признается время, хранящееся в поле notAfter поля Validity сертификата ключа подписи. В данном случае информация об аннулированном сертификате ключа подписи Оператора Удостоверяющего центра в список отозванных сертификатов не заносится.

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра временем аннулирования сертификата ключа подписи Оператора 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 Оператора Удостоверяющего центра в список отозванных сертификатов не заносится.

8.5.1. Аннулирование (отзыв) сертификата ключа подписи Оператора Удостоверяющего центра по заявлению Оператора Удостоверяющего центра

Подача заявления на аннулирование (отзыв) сертификата ключа подписи осуществляется Оператором Удостоверяющего центра посредством почтовой или курьерской связи по форме Приложения № 8.

После получения Удостоверяющим центром заявления на аннулирование (отзыв) сертификата ключа подписи Администратор Удостоверяющего центра

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

В случае отказа в отзыве сертификата ключа подписи Удостоверяющий центр уведомляет об этом Оператора Удостоверяющего центра.

При принятии положительного решения Администратор Удостоверяющего центра отзывает сертификат ключа подписи Оператора Удостоверяющего центра.

8.5.2. Аннулирование (отзыв) сертификата ключа подписи Оператора Удостоверяющего центра по заявлению на отзыв доверенности

Оператор предоставления услуг Удостоверяющего центра вправе отозвать сертификаты ключей подписей своих полномочных представителей – Операторов Удостоверяющего центра, путем подачи заявления на отзыв доверенности Оператора Удостоверяющего центра.

Форма заявления на отзыв доверенности приведена в Приложении №9 к настоящему Регламенту.

После получения Удостоверяющим центром заявления на отзыв доверенности Оператора Удостоверяющего центра Администратор Удостоверяющего центра осуществляет ее рассмотрение и обработку. Обработка заявления на отзыв доверенности должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в отзыве сертификатов ключей подписей Удостоверяющий центр уведомляет об этом Оператора предоставления услуг Удостоверяющего центра.

При принятии положительного решения Администратор Удостоверяющего центра отзывает сертификаты ключей подписей Оператора Удостоверяющего центра.

8.6. Приостановление действия сертификата ключа подписи Оператора Удостоверяющего центра

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

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

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

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

8.6.1. Приостановление действия сертификата ключа подписи Оператора Удостоверяющего центра по заявлению в бумажной форме

Заявление на приостановление действия сертификата ключа подписи Оператора Удостоверяющего центра оформляется по форме Приложения № 10 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

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

В случае отказа в приостановлении действия сертификата ключа подписи Удостоверяющий центр уведомляет об этом Оператора Удостоверяющего центра.

При принятии положительного решения Администратор Удостоверяющего центра приостанавливает действие сертификата ключа подписи Оператора Удостоверяющего центра.

8.6.2. Приостановление действия сертификата ключа подписи Оператора Удостоверяющего центра по заявлению в устной форме

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

Заявление подается в Удостоверяющий центр по телефону.

Оператор Удостоверяющего центра должен сообщить Администратору Удостоверяющего центра следующую информацию:

- идентификационные данные, содержащиеся в сертификате ключа подписи, действие которого необходимо приостановить;
- серийный номер сертификата ключа подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа подписи;

– ключевую фразу Оператора Удостоверяющего центра (ключевая фраза определяется в процессе регистрации Оператора Удостоверяющего центра).

Заявление Удостоверяющим центром принимается только в случае положительной аутентификации Оператора Удостоверяющего центра (совпадения ключевой фразы, переданной в заявлении с информацией из реестра зарегистрированных пользователей Удостоверяющего центра).

После принятия заявления Администратор Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа подписи. Принятие решения о приостановлении действия сертификата должно быть осуществлено в течение рабочего дня поступления данного заявления.

В случае отказа в приостановлении действия сертификата ключа подписи Оператор Удостоверяющего центра уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Администратор Удостоверяющего центра приостанавливает действие сертификата открытого ключа.

Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата ключа подписи Оператор Удостоверяющего центра должен предоставить в Удостоверяющий центр заявление на аннулирование (отзыв) сертификата ключа подписи в бумажной форме (в том случае, если факт компрометации закрытого ключа подтвердился), либо заявление на возобновление действия сертификата ключа подписи (в том случае, если компрометации закрытого ключа не было).

8.6.3. Приостановление действия сертификата ключа подписи по решению Удостоверяющего центра

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

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

8.7. Возобновление действия сертификата ключа подписи Оператора Удостоверяющего центра

Удостоверяющий центр возобновляет действие сертификата ключа подписи Оператора Удостоверяющего центра только по заявлению Оператора Удостоверяющего центра.

Подача заявления на возобновление действия сертификата ключа подписи осуществляется Оператором Удостоверяющего центра посредством почтовой или курьерской связи по форме Приложения № 11.

Возобновление действия сертификата ключа подписи и официальное уведомление Оператора и всех лиц, зарегистрированных в Удостоверяющем центре о возобновлении действия сертификата ключа подписи должны быть осуществлены не позднее 5-ти рабочих дней следующих за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

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 возможно только в течение срока, на который действие сертификата ключа подписи было приостановлено.

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

Получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром осуществляется на основании заявления, направляемого Оператором Удостоверяющего центра. Данное заявление оформляется по форме Приложения №12 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 Оператору Удостоверяющего центра.

Предоставление Оператору Удостоверяющего центра справки о статусе сертификата ключа подписи должно быть осуществлено не позднее десяти рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

8.9. Подтверждение подлинности электронной цифровой подписи в электронном документе

По желанию Оператора предоставления услуг Удостоверяющего центра (Уполномоченной Организации), Удостоверяющий центр осуществляет проведение

экспертных работ по подтверждению 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 Оператор удостоверяющего центра подает заявление в Удостоверяющий центр по форме, приведенной в Приложении №13.

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 Оператором предоставления услуг Удостоверяющего центра (Уполномоченной Организацией). 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).

8.10. Регистрация и управление сертификатами ключей подписей Пользователей Удостоверяющего центра

Регистрация Пользователей Удостоверяющего центра, принятие решений по изготовлению сертификатов ключей подписей и управлению сертификатами ключей подписей, формирование копий сертификатов ключей подписей Пользователей Удостоверяющего центра производится Оператором Удостоверяющего центра и осуществляется в соответствии с порядком, установленным Уполномоченной Организацией.

Удостоверяющий центр выполняет действия по изготовлению сертификатов ключей подписей, отзыву сертификатов ключей подписей, приостановлению и возобновлению действий сертификатов ключей подписей на основании заявлений в электронной форме, подписанных ЭЦП, и направляемых Оператором Удостоверяющего центра с использованием АРМ администратора ЦР. Выполнение указанных действий осуществляется Удостоверяющим центром при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭЦП Оператора Удостоверяющего центра;
- Сертификат ключа подписи Оператора Удостоверяющего центра на момент получения заявления Удостоверяющим центром действителен;
- Закрытый ключ подписи Оператора Удостоверяющего центра на момент формирования ЭЦП заявления действителен;
- Сертификат ключа подписи Оператора Удостоверяющего центра содержит в расширении Extended Key Usage область использования – Оператор Центра Регистрации (1.2.643.2.2.34.5).

8.11. 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 центров 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.

8.12. Прочие условия

8.12.1. Регистрация Оператора в Удостоверяющем центре и подача заявления на изготовление сертификата ключа подписи Оператора Удостоверяющего центра может быть осуществлена уполномоченным представителем Оператора Удостоверяющего центра, действующим на основании соответствующим образом оформленной доверенности. Форма доверенности на осуществление регистрации Оператора в Удостоверяющем центре и получения ключей подписей и сертификата ключа подписи Оператора Удостоверяющего центра приведена в Приложении № 4 настоящего Регламента.

9. Структура сертификатов ключей подписей и сроки действия ключевых документов

9.1. 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 UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
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 Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SybjectType (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

9.2. Структура сертификата ключа подписи Оператора 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	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по (notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество OrganizationUnit = Подразделение Organization = Организация Locality = Город Country = Страна = RU E = Электронная почта Компонента имени CN и O обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата
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
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Оператор Центра Регистрации - (1.2.643.2.2.34.5) Проверка подлинности клиента - (1.3.6.1.5.5.7.3.2)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/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

9.3. 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 UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
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 и Оператором Удостоверяющего центра. 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	Улучшеный 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 Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/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 и RFC 5280

9.4. 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 UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
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 и Оператором Удостоверяющего центра. 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	Улучшеный 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 Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/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 и RFC 5280

9.5. 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 UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "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

9.6. Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи содержат сведения об отношениях, при осуществлении которых электронный документ, подписанный ЭЦП, будет иметь юридическое значение. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре и определяющих отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение приведен в Приложении № 1 настоящего Регламента.

9.7. Сроки действия ключевых документов

9.7.1. 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.

9.7.2. Срок действия закрытого ключа Оператора Удостоверяющего центра составляет 1 (один) год.

Начало периода действия закрытого ключа Оператора Удостоверяющего центра исчисляется со времени начала действия соответствующего сертификата ключа подписи.

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

9.7.3. Срок действия закрытого ключа Пользователя Удостоверяющего центра 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.

10. Дополнительные положения

10.1. Плановая смена ключей Уполномоченного лица Удостоверяющего Центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Уполномоченного лица Удостоверяющего центра выполняется в период 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.

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.

По истечении одного года с момента проведения плановой смены ключей Уполномоченного лица Удостоверяющий центр изготавливает список отозванных сертификатов, соответствующий старому закрытому ключу, со сроком действия соответствующим сроку действия старого сертификата Уполномоченного лица Удостоверяющего центра (значение поля nextUpdate списка отозванных сертификатов совпадает со значением поля notAfter поля Validity сертификата ключа подписи Уполномоченного лица Удостоверяющего центра). Изданный список отозванных сертификатов публикуется Удостоверяющим центром, изготовление нового списка отозванных сертификатов, соответствующего старому закрытому ключу Уполномоченного лица Удостоверяющего центра, более не осуществляется.

10.2. 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), Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты, изданные с использованием скомпрометированного ключа Уполномоченного лица Удостоверяющего центра, считаются аннулированными.

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 10.1 настоящего Регламента).

Все действовавшие на момент компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра сертификаты ключей подписей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

10.3. Компрометация ключевых документов Оператора Удостоверяющего центра

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

В случае компрометации или угрозы компрометации закрытого ключа Оператор связывается с Администратором Удостоверяющего центра по телефону и приостанавливает действие сертификата, соответствующего скомпрометированному ключу, посредством подачи заявления на приостановление действие сертификата в устной форме (пункт 8.6.2 настоящего Регламента).

Оператор Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 8.4 настоящего Регламента.

10.4. Конфиденциальность информации

10.4.1. Типы конфиденциальной информации

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

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

10.4.2. Типы информации, не являющейся конфиденциальной

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

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

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

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

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

10.4.3. Исключительные полномочия Удостоверяющего центра

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

10.5. Хранение сертификатов ключей подписей в Удостоверяющем центре

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

10.6. Прекращение оказания услуг Удостоверяющим центром

10.6.1. В случае прекращения действия настоящего Регламента в отношении Оператора предоставления услуг Удостоверяющего центра (Уполномоченной организации) все сертификаты ключей подписей, владельцами которых являются Операторы Удостоверяющего центра и Пользователи Удостоверяющего центра, зарегистрированные данными Операторами Удостоверяющего центра, аннулируются (отзываются) Удостоверяющим центром.

10.7. Форс-мажор

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

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

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

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

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

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

11. Список приложений

11.1. Приложение №1. 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

11.2. Приложение №2. Форма заявления на регистрацию Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

11.3. Приложение №3. Форма доверенности Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

11.4. Приложение №4. Форма доверенности на предоставление заявительных документов и получения ключей подписей и сертификата Оператора Удостоверяющего центра

11.5. Приложение №5. Форма заявления на изготовление сертификата ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (при генерации ключей подписей в Удостоверяющем центре)

11.6. Приложение №6. Форма заявления на изготовление сертификата ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (при генерации ключей подписи на рабочем месте Оператора с использованием АРМ администратора ЦР)

11.7. Приложение №7. Форма заявления на изготовление сертификата ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (при генерации ключей подписей на рабочем месте Оператора посредством веб-интерфейса, предоставляемого Удостоверяющим центром)

11.8. Приложение №8. Форма заявления на аннулирование (отзыв) сертификата ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

11.9. Приложение №9. Форма заявления на отзыв доверенности Оператора Удостоверяющего Центра ООО «КРИПТО-ПРО»

11.10. Приложение №10. Форма заявления на приостановление действия сертификата ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

11.11. Приложение №11. Форма заявления на возобновление действия сертификата ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

11.12. Приложение №12. Форма заявления на получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром ООО «КРИПТО-ПРО»

11.13. Приложение №13. Форма заявления на подтверждение подлинности электронной цифровой подписи в электронном документе

11.14. Приложение №14. Форма печати копии сертификата ключа подписи, издаваемого Удостоверяющим центром ООО «КРИПТО-ПРО»

Приложение №1 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»

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

	OID	Область применения
1.	1.2.643.2.2.34.5	Оператор Центра Регистрации – формирование электронной цифровой подписи электронных документов, определенных Регламентом для Оператора 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

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

Заявление на регистрацию Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит зарегистрировать уполномоченного представителя

_____
(фамилия, имя, отчество)

в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО» и наделить полномочиями Оператора Удостоверяющего центра ООО «КРИПТО-ПРО», установленными Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО».

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.

Подпись уполномоченного представителя организации _____ /_____/
«____» _____ 20____ г.

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

Приложение №3 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма доверенности Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

выступать в роли Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» и осуществлять действия в рамках Регламента Удостоверяющего центра ООО «КРИПТО-ПРО», установленные для Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».
Представитель наделяется правом расписываться в соответствующих документах Удостоверяющего центра ООО «КРИПТО-ПРО» для исполнения поручений, определенных настоящей Доверенностью.

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

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

подтверждаю.

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

Приложение №4 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма доверенности на предоставление заявительных
документов и получения ключей подписей и сертификата
Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

1. Предоставить в Удостоверяющий центр ООО «КРИПТО-ПРО» необходимые документы и средства, определенные Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО» для регистрации, генерации ключей и изготовления сертификата ключа подписи своего полномочного представителя - Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»)

2. Получить необходимые лицензии на право пользования программного обеспечения для Оператора Удостоверяющего центра ООО «КРИПТО-ПРО», сертификат ключа подписи Уполномоченного лица Удостоверяющего центра ООО «КРИПТО-ПРО» и иные документы, определенные Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО»

3. Получить сформированный ключевой носитель, содержащий закрытый ключ подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»)

Приложение №4 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма доверенности на предоставление заявительных
документов и получения ключей подписей и сертификата
Оператора Удостоверяющего центра)

Представитель наделяется правом расписываться в сертификате ключа подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» на бумажном носителе и в соответствующих документах Удостоверяющего центра ООО «КРИПТО-ПРО» для исполнения поручений, определенных настоящей доверенностью.

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

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

Оператор Удостоверяющего центра
ООО «КРИПТО-ПРО» _____ /_____/
(Подпись) (Фамилия И.О. Оператора)

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

Приложение №5 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на изготовление сертификата
при генерации ключей подписей в Удостоверяющем центре)

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит сформировать ключи подписи, записать сформированный закрытый ключ подписи на предоставленный ключевой носитель и изготовить сертификат ключа подписи своего уполномоченного представителя – Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)[1]	Фамилия, Имя, Отчество или псевдоним	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Organization Unit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Contry (C)	RU	
Extended Key Usage	Проверка подлинности клиента Оператор Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.2.643.2.2.34.5)

Оператор Удостверяющего центра
ООО «КРИПТО-ПРО» _____ /_____/
«____» _____ 20____ г.

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

[1] - Обязательными для заполнения полями (расширениями) являются Common Name (CN) и Extended Key Usage. Необходимость установления значений остальных полей определяется заявителем

Приложение №6 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на изготовление сертификата при генерации ключей
подписей на рабочем месте Оператора Удостоверяющего центра
с использованием АРМ администратора ЦР)

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит изготовить сертификат ключа подписи своего уполномоченного представителя – Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)[1]	Фамилия, Имя, Отчество или псевдоним	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Organization Unit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Contry (C)	RU	
Extended Key Usage	Проверка подлинности клиента Оператор Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.2.643.2.2.34.5)

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

Приложение №6 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на изготовление сертификата при генерации ключей
подписей на рабочем месте Оператора Удостоверяющего центра
с использованием АРМ администратора ЦР)

и сформированным запросом на сертификат ключа подписи формата PKCS#10 в кодировке Base64.

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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC4jCCAo8CAQAwgYAxITAfBgkqhkiG9w0BCQEWEml2YW5vdkBtLXJlZXN0ci5y
dTELMAkGA1UEBhMCUlUxDzANBgNVBAcTBk1vc2NvdzEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMQ0wCwYDVQQLEwREZXB0MRcwFQYDVQQDEw5JdmFuIEkuIEl2YW5vdjBj
MBwGBiqFAwICEzASBgcqhQMCAiQABgcqhQMCAh4BA0MABEBog51WRaScCe7qMJ3g
2s+zrO8y4G5VhcaIdxWIYKWmcHL8AHKGC2pmOWCmE/XzUZorhycAYrUaH0gstA9C
nz17oIIBoDAaBgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwYwYKKwYBBAGCNwIB
DjFVMFMwDgYDVR0PAQH/BAQDAgTwMBkGCSqGSIb3DQEJDwQMMAowCAYGKoUDAgIV
MCYGA1UdJQQfMB0GCCsGAQUFBwMCBggrBgEFBQcDBAYHKoUDAgIiBjCCARsGCisG
AQQBgjcNAgIxggELMIIBBwIBAR52AEMAcgB5AHAAdABvAC0AUAByAG8AIABHAE8A
UwBUACAAUgAgADMANAAuADEAMAAtADIAMAAwADEAIABDAHIAeQBwAHQAbwBnAHIA
YQBwAGgAaQBjACAAUwBlAHIAdgBpAGMAZQAgAFAAcgBvAHYAaQBkAGUAcgOBiQAk
ofCLPzGSbmXMEex/cq9WymQT+3kQlCRX0bRnOsMlGVV4AxJLfMS5x1PX/wWKxIv9
vnjdFdnXcklLJ5cw8g9kkpMzdNEcEMgPYEi0xttZ9r3aTsIEjBEn7+1h8IgY+yDy
deR9DgPvC/QFS0diXCWYESkt2PiiAyAY/4WmVS1NSwAAAAAAAAAAMAoGBiqFAwIC
AwUAA0EAixD6RSeDYbF/VVjPfi+H+klhKaz5MbFNRa9BVIViFS3ccRvNZVpEfUFx
HriROkQQa3/9hfEWRAupRwMye/3CMg==
-----END NEW CERTIFICATE REQUEST-----
```

Оператор Удостверяющего центра
ООО «КРИПТО-ПРО» _____ /_____/
«____» _____ 20____ г.

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

Приложение №7 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на изготовление сертификата при генерации ключей подписей на рабочем месте Оператора Удостоверяющего центра посредством веб-интерфейса, предоставляемого Удостоверяющим центром)

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

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 34.10-2001
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: Оператор Центра Регистрации(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
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 34.10-2001 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 34.11/34.10-2001
Параметры: 0500
Значение: BABC 1455 ADA3 DC7F 0EC9 3A1A 5020 C0DE F561 C757 2986 BB2E B180 A5B0 091A 7F0A 6FA1 1A6E EE48 A366 B904 7288 A311 D966 BB2F FC7C EB75 3F0A 49ED A651 3E10 258A

Оператор 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»
(Форма заявления на аннулирование (отзыв) сертификата)

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

в связи с _____
(причина отзыва сертификата)

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

содержащий следующие идентификационные данные:

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

Подпись владельца сертификата ключа подписи – Оператора Удостверяющего 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»
(Форма заявления на отзыв доверенности)

Заявление на отзыв доверенности

_____
(наименование организации, включая организационно-правовую форму)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Заявляет, что отзывает Доверенность №_____ от «_____» _____ 20___ года, выданную для представления в Удостоверяющий центр ООО «КРИПТО-ПРО» своему полномочному представителю – Оператору Удостоверяющего Центра ООО «КРИПТО-ПРО» _____
(фамилия, имя, отчество)

и просит аннулировать (отозвать) сертификаты ключей подписей, содержащие область использования - Оператор Центра Регистрации (1.2.643.2.2.34.5), владельцем которых является данный Оператор Удостоверяющего центра ООО «КРИПТО-ПРО».

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

Приложение №10 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на приостановление действия сертификата)

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

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

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

Подпись владельца сертификата ключа подписи – Оператора Удостверяющего центра ООО «КРИПТО-ПРО» _____ /_____/
«____» _____ 20____ г.

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

Приложение №11 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на возобновление действия сертификата)

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

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

Подпись владельца сертификата ключа подписи – Оператора Удостверяющего центра ООО «КРИПТО-ПРО» _____ /_____/
«____» _____ 20____ г.

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

Приложение №12 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на получение информации о статусе сертификата)

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

Оператор Удостоверяющего центра ООО «КРИПТО-ПРО» - полномочный представитель

_____

(полное наименование организации, включая организационно-правовую форму)

Просит предоставить информацию о статусе следующего сертификата ключа подписи:

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

Время[3] (период времени) на момент наступления которого требуется установить статус сертификата: «_____» по «_____».

Оператор Удостоверяющего центра
ООО «КРИПТО-ПРО» _____/_____/
«____» _____ 20____ г.

[3] 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 №13 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на подтверждение подлинности ЭЦП)

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. Время[4] на момент наступления которых требуется подтвердить подлинность ЭЦП: «_____:_____» «_____/_____/_____»;
час минута день месяц год

Оператор Удостоверяющего центра
ООО «КРИПТО-ПРО» _____/_____/
«____» _____ 20____ г.

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

[4] 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 №14 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма печати копии сертификата ключа подписи)

Копия сертификата ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан:
Фамилия Имя Отчество
Кем выдан:
CryptoPro CA
Действителен с 15 октября 2003 г. 12:03:00 UTC по 15 октября 2004 г. 12:12:00 UTC
Версия: 3 (0x2)
Серийный номер: 14F5 9CF2 0000 0000 003A
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Издатель сертификата: CN = CryptoPro CA, C = 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 = User1
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: Оператор Центра Регистрации(1.2.643.2.2.34.5) 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=50AA 3E1E 4186 F8DC 3585 6E11 2C11 D9E3 0A91 7AD7 Поставщик сертификата: Адрес каталога: CN=CryptoPro CA C=RU Серийный номер сертификата=29D1 B0C8 C311 ACAE 48DB AAB1 3687 CEFC
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 уполномоченного лица УЦ: _____/_____

«____» _____ 20__ г.

Печать Удостоверяющего Центра

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.