

Утвержден
Приказом ООО «КРИПТО-ПРО»
от «12» апреля 2012 г. № 2

РЕГЛАМЕНТ
Центра управления сертификатами VPN-сетей
(ЦУС VPN)
(Схема обслуживания: распределенная с оператором)

Редакция № 1

г. Москва
2012

1. Сведения о Центре управления сертификатами VPN-сетей

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дальнейшем «Центр управления сертификатами VPN-сетей» («ЦУС VPN»), зарегистрировано на территории Российской Федерации в городе Москва (Свидетельство о регистрации № 001.602.749 выдано 16.11.1999 г. Государственным учреждением Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003 г.).

ЦУС VPN 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, корп. 50

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

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

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

- 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) 780-48-20; e-mail: vpnca@cryptopro.ru

2. Термины и определения

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

Администратор ЦУС VPN – ответственный сотрудник ЦУС VPN, наделенный ЦУС VPN полномочиями по осуществлению действий по регистрации и управлению сертификатами открытых ключей Операторов ЦУС VPN.

Владелец сертификата открытого ключа – физическое лицо, на имя которого ЦУС VPN выдан сертификат открытого ключа и которое владеет соответствующим закрытым ключом.

Закрытый ключ - уникальная последовательность символов, известная владельцу сертификата открытого ключа и предназначенная для формирования электронной подписи данных и расшифрования данных.

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

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

Личный кабинет в ЦУС VPN – закрытый информационный профиль Оператора или Пользователя в Web-интерфейсе ЦУС VPN, доступ в который может быть осуществлен только посредством аутентификации по действующему сертификату открытого ключа и соответствующему ему закрытому ключу.

Маркер временного доступа - идентификатор (десятичное число) и секретный пароль (пятизначное символьное значение), предоставляющиеся Пользователю и Оператору ЦУС VPN, не имеющим действующего закрытого ключа, для формирования и передачи в ЦУС VPN запроса на сертификат открытого ключа посредством Web-интерфейса, предоставляемого ЦУС VPN.

Оператор предоставления услуг ЦУС VPN, Уполномоченная Организация – юридическое лицо, заключившее с ЦУС VPN договор на предоставление услуг по изготовлению сертификатов открытых ключей и уполномоченное ЦУС VPN осуществлять регистрацию и управление сертификатами открытых ключей ЦУС VPN.

Оператор ЦУС VPN – физическое лицо, являющееся сотрудником Уполномоченной Организации, наделенное ЦУС VPN и Уполномоченной Организацией правами по осуществлению действий по регистрации и управлению сертификатами открытых ключей Пользователей ЦУС VPN.

Открытый ключ - уникальная последовательность символов, соответствующая закрытому ключу, предназначенная для проверки электронной подписи данных и шифрования данных.

Подтверждение подлинности электронной подписи электронного документа – положительный результат проверки СКЗИ с использованием сертификата открытого ключа принадлежности электронной подписи владельцу сертификата и отсутствия изменений в электронном документе после момента его подписания.

Пользователь ЦУС VPN – физическое лицо, зарегистрированное в ЦУС VPN и являющееся владельцем сертификата открытого ключа, изданного ЦУС VPN.

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

Сертификат открытого ключа - электронный документ с электронной подписью уполномоченного лица ЦУС VPN, структура которого определяется настоящим Регламентом и который изготавливается ЦУС VPN для подтверждения идентификации владельца сертификата открытого ключа, обеспечения его аутентификации, электронной подписи и шифрования данных. Сертификат открытого ключа действует на определенный момент времени (действующий сертификат) если:

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

Сканирование бумажного документа - создание электронного образа бумажного документа с помощью специальных средств, обеспечивающих преобразование изображения на бумажном носителе в цифровую форму. Результатом сканирования бумажного документа является файл, содержащий растровое графическое изображение данного бумажного документа.

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

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники – СКЗИ «КриптоПро CSP», осуществляющее криптографические преобразования информации для обеспечения ее безопасности. ЦУС VPN осуществляет формирование закрытых ключей и изготовление сертификатов открытых ключей с использованием СКЗИ «КриптоПро CSP».

Центр управления сертификатами VPN-сетей (ЦУС VPN) – ООО «КРИПТО-ПРО», осуществляющее выполнение следующих целевых функций:

- изготавливает сертификаты открытых ключей;
- создает закрытые ключи с гарантией сохранения их в тайне;
- приостанавливает и возобновляет действие сертификатов открытых ключей, а также аннулирует их;
- проверяет уникальность открытых ключей;
- выдает сертификаты открытых ключей с информацией об их действии.

Уполномоченное лицо ЦУС VPN – физическое лицо, являющееся сотрудником ЦУС VPN и наделенное ЦУС VPN полномочиями по заверению сертификатов открытых ключей и списков отозванных сертификатов.

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

Base 64 – способ кодирования, обеспечивающий представление произвольных бинарных данных с использованием печатных символов.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. ЦУС VPN

осуществляют свою работу в соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

VPN-сеть – Virtual Private Network, виртуальная частная сеть, обеспечивающая с использованием Средства криптографической защиты информации целостность и конфиденциальность передаваемых в данной сети данных, а при необходимости аутентификацию участников данной сети и авторство передаваемых данных.

Web-интерфейс, предоставляемый ЦУС VPN – интерфейс взаимодействия ЦУС VPN с Пользователем и Оператором ЦУС VPN, предназначенный для управления сертификатами открытых ключей реализованный в виде набора Web-страниц и размещенный на Web-узле ЦУС VPN.

3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент Центра управления сертификатами VPN-сетей (ЦУС VPN) (Схема обслуживания: распределенная с оператором), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации.

3.1.2. Сторонами Регламента (далее Стороны) являются ЦУС VPN – ООО «КРИПТО-ПРО» и Оператор предоставления услуг ЦУС VPN (Уполномоченная Организация).

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

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 ЦУС VPN в одностороннем порядке.

3.3.2. Уведомление о внесении изменений (дополнений) в Регламент осуществляется ЦУС VPN путем обязательного размещения указанных изменений (дополнений) на сайте ЦУС VPN по адресу – http://vpnca.cryptopro.ru/reglament/reglamentoper_vpnca.pdf.

3.3.3. Все изменения (дополнения), вносимые ЦУС VPN 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 ЦУС VPN.

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, заключивших договор на оказание услуг ЦУС VPN, в том числе заключивших договор 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. ЦУС VPN предоставляет Оператору предоставления услуг ЦУС VPN по его требованию:

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

4.2. Уполномоченная Организация предоставляет ЦУС VPN по его требованию документы, подтверждающие следующую информацию:

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

5. Права и обязанности сторон

5.1. ЦУС VPN обязан:

- 5.1.1. Предоставить Оператору ЦУС VPN сертификат уполномоченного лица ЦУС VPN.
- 5.1.2. Использовать для изготовления закрытого ключа уполномоченного лица ЦУС VPN и для выполнения криптографических операций только сертифицированные в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации.
- 5.1.3. Использовать закрытый ключ уполномоченного лица ЦУС VPN только для подписи издаваемых им сертификатов открытых ключей и списков отозванных сертификатов.
- 5.1.4. Принять меры по защите закрытого ключа уполномоченного лица ЦУС VPN от несанкционированного доступа.
- 5.1.5. Организовать свою работу по Всемирному координированному времени (Coordinated Universal Time, UTC) с учетом часового пояса города Москвы. ЦУС VPN обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.
- 5.1.6. Изготовить сертификат открытого ключа Оператора в ЦУС VPN по заявлению на изготовление сертификата в соответствии с порядком, определенным в настоящем Регламенте.
- 5.1.7. Обеспечить занесение регистрационной информации Пользователя ЦУС VPN в реестр ЦУС VPN и обеспечить уникальность регистрационной информации всех зарегистрированных в ЦУС VPN лиц, используемой для идентификации владельцев сертификатов открытых ключей.
- 5.1.8. Обеспечить изготовление сертификата открытого ключа Пользователя ЦУС VPN, в соответствии с порядком, определенным в настоящем Регламенте.
- 5.1.9. Обеспечить уникальность серийных номеров изготавливаемых сертификатов открытых ключей.
- 5.1.10. Обеспечить уникальность значений открытых ключей в изготовленных сертификатах открытых ключей.
- 5.1.11. Аннулировать (отозвать), приостановить и возобновить действие сертификата открытого ключа Оператора ЦУС VPN по соответствующему заявлению на аннулирование (отзыв), приостановление и возобновление действия сертификата открытого ключа, в соответствии с порядком, определенным в настоящем Регламенте.
- 5.1.12. Обеспечить аннулирование (отзыв), приостановление и возобновление действия сертификата открытого ключа Пользователя ЦУС VPN в соответствии с порядком, определенным в настоящем Регламенте.
- 5.1.13. Аннулировать (отозвать) сертификат открытого ключа Оператора и Пользователя ЦУС VPN, если истек установленный срок, на который действие данного сертификата было приостановлено.
- 5.1.14. Аннулировать (отозвать) сертификат открытого ключа Оператора и Пользователя ЦУС VPN в случае компрометации закрытого ключа уполномоченного лица ЦУС VPN, с использованием которого был издан сертификат открытого ключа.
- 5.1.15. Уведомить установленным настоящим Регламентом образом об аннулировании (отзыве), приостановлении и возобновлении действия сертификата открытого ключа всех лиц, зарегистрированных в ЦУС VPN.

5.1.16. Публиковать актуальный список отозванных сертификатов на сайте ЦУС VPN. Период публикации списка отозванных сертификатов в рабочее время ЦУС VPN – 1 (Один) час.

5.1.17. Предоставить Уполномоченной Организации необходимые средства и права по осуществлению регистрации пользователей в ЦУС VPN, изготовлению и управлению сертификатами открытых ключей Пользователей ЦУС VPN.

5.2. Уполномоченная Организация (Оператор предоставления услуг ЦУС VPN) обязана:

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

5.2.2. Оператор ЦУС VPN, являющийся полномочным представителем Уполномоченной Организации обязан:

5.2.2.1. Формировать личные открытые и закрытые ключи только с использованием средства криптографической защиты информации и программного обеспечения, предоставленного ЦУС VPN.

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 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. Немедленно обратиться в ЦУС VPN, с заявлением на приостановление действия сертификата открытого ключа в случае потери, раскрытия, искажения личного закрытого ключа.

5.2.2.6. Не использовать личный закрытый ключ, связанный с сертификатом открытого ключа, заявление на аннулирование (отзыв) которого подано в ЦУС VPN, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата в ЦУС VPN по момент времени официального уведомления об аннулировании (отзыве) сертификата, либо об отказе в аннулировании (отзыве).

5.2.2.7. Не использовать личный закрытый ключ, связанный с сертификатом открытого ключа, заявление на приостановление действия которого подано в ЦУС VPN, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в ЦУС VPN по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

5.3. ЦУС VPN имеет право:

5.3.1. Отказать в изготовлении сертификата открытого ключа Оператора ЦУС VPN в случае ненадлежащего оформления заявления на изготовление сертификата открытого ключа.

5.3.2. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата открытого ключа Оператора ЦУС VPN в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв), приостановление и возобновление действия сертификата открытого ключа.

5.3.3. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата открытого ключа Оператора и Пользователя ЦУС VPN в случае, если истек установленный срок действия закрытого ключа, соответствующего сертификату.

5.3.4. По согласованию с Уполномоченной Организацией приостановить действие сертификата открытого ключа Оператора и Пользователя ЦУС VPN с обязательным уведомлением владельца сертификата открытого ключа, действие которого приостановлено, и указанием обоснованных причин.

5.3.5. Отказать в изготовлении сертификата открытого ключа Оператора и Пользователя ЦУС VPN в случае, если использованное Оператором и Пользователем ЦУС VPN для формирования запроса на сертификат открытого ключа средство криптографической защиты информации не поддерживается ЦУС VPN.

5.4. Оператор ЦУС VPN и Пользователь ЦУС VPN имеют право:

5.4.1. Применять сертификат открытого ключа ЦУС VPN для проверки электронной подписи уполномоченного лица ЦУС VPN в сертификатах открытых ключей, изготовленных ЦУС VPN.

5.4.2. Применять список отозванных сертификатов открытых ключей, изготовленный ЦУС VPN, для установления статуса сертификатов открытых ключей, изданных ЦУС VPN.

5.4.3. Для хранения личного закрытого ключа применять любой носитель, поддерживаемый средством криптографической защиты информации.

5.4.4. Оператор ЦУС VPN имеет право:

5.4.4.1. Обратиться в ЦУС VPN с заявлением на изготовление сертификата открытого ключа.

5.4.4.2. Обратиться в ЦУС VPN с заявлением на аннулирование (отзыв) и приостановление действия сертификата открытого ключа, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

5.4.4.3. Обратиться в ЦУС VPN с заявлением на возобновление действия сертификата открытого ключа, владельцем которого он является, в течение срока действия соответствующего закрытого ключа и срока, на который действие сертификата было приостановлено.

5.4.4.4. Регистрировать в ЦУС VPN пользователей и заносить регистрационную информацию в реестр ЦУС VPN.

5.4.4.5. Принимать по заявлению на изготовление сертификата открытого ключа Пользователя ЦУС VPN решение по изготовлению сертификата открытого ключа.

5.4.4.6. Аннулировать (отзывать) сертификат открытого ключа Пользователя ЦУС VPN в течение срока действия соответствующего данному сертификату закрытого ключа.

5.4.4.7. Приостанавливать действие сертификата открытого ключа Пользователя ЦУС VPN в течение срока действия соответствующего данному сертификату закрытого ключа.

5.4.4.8. Возобновлять действие сертификата открытого ключа Пользователя ЦУС VPN в течение срока действия соответствующего данному сертификату закрытого ключа и срока, на который действие сертификата было приостановлено.

5.4.5. Пользователь ЦУС VPN имеет право:

5.4.5.1. Воспользоваться предоставляемыми ЦУС VPN программными средствами для передачи по линиям связи в ЦУС VPN заявления на изготовление сертификата открытого ключа в электронном виде.

5.4.5.2. Воспользоваться предоставляемыми ЦУС VPN программными средствами для передачи по линиям связи в ЦУС VPN заявлений на аннулирование (отзыв), приостановление и возобновление действия сертификата открытого ключа в электронном виде.

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

6.4. ЦУС VPN несет ответственность за убытки при использовании закрытого ключа и сертификата открытого ключа Пользователя и Оператора ЦУС VPN только в случае, если данные убытки возникли при компрометации закрытого ключа уполномоченного лица ЦУС VPN.

6.5. Вся ответственность по регистрации Пользователей ЦУС VPN, занесению данных в сертификаты открытых ключей, принятию решений по изготовлению и управлению сертификатами открытых ключей Пользователей ЦУС VPN полностью возлагается на Оператора ЦУС VPN, являющегося полномочным лицом Уполномоченной Организации (Оператора предоставления услуг ЦУС VPN).

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 ЦУС VPN - ООО «КРИПТО-ПРО» и Уполномоченная Организация (Оператор предоставления услуг ЦУС VPN).

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 ЦУС VPN

8.1. Изготовление сертификата открытого ключа Оператора ЦУС VPN

Изготовление сертификата открытого ключа Оператора ЦУС VPN может быть осуществлено при личном прибытии Оператора, либо его полномочного представителя, в ЦУС VPN (формирование закрытых ключей осуществляется непосредственно в ЦУС VPN), посредством Web-интерфейса, предоставляемого ЦУС VPN, либо на основании файла запроса на изготовление сертификата открытого ключа в электронной форме.

8.1.1. Изготовление сертификата открытого ключа Оператора ЦУС VPN при личном прибытии Оператора, либо его полномочного представителя, в ЦУС VPN.

Изготовление сертификата открытого ключа Оператора ЦУС VPN при личном прибытии Оператора, либо его полномочного представителя, в ЦУС VPN осуществляется на основании заявления на изготовление сертификата. Форма заявления на изготовление сертификата приведена в Приложении № 1 настоящего Регламента.

На Оператора ЦУС VPN должна быть оформлена доверенность, уполномочивающая его выступать в роли Оператора ЦУС VPN и совершать действия, определенные положениями настоящего Регламента для Оператора ЦУС VPN. Указанная доверенность оформляется по форме Приложения № 2 настоящего Регламента.

В случае прибытия полномочного представителя Оператора в ЦУС VPN, указанный представитель должен предоставить доверенность на получение закрытых ключей и сертификата за Оператора ЦУС VPN по форме Приложения №3 настоящего Регламента.

Приведенные заявительные документы, а также носитель для записи ключевой информации, должны быть предоставлены Администратору ЦУС VPN.

Администратор ЦУС VPN на основе полученных заявительных документов выполняет действия по формированию закрытого ключа на предоставленный носитель, изготовлению сертификата открытого ключа, записи сертификата открытого ключа на предоставленный носитель, после чего предоставляет прибывшему лицу носитель, содержащий закрытый ключ и сертификат открытого ключа Оператора ЦУС VPN.

После выполнения указанных действий Администратор ЦУС VPN распечатывает информацию, содержащуюся в изданном сертификате, которая подписывается прибывшим лицом собственноручной подписью, что свидетельствует о следующем:

- данные, содержащиеся в изданном сертификате открытого ключа соответствуют данным, указанным в заявлении на изготовление сертификата;
- закрытый ключ, записанный на носителе и соответствующий изданному сертификату, Администратором ЦУС VPN передан, а прибывшим лицом - получен.

Изготовление сертификата открытого ключа при личном прибытии Оператора, либо его полномочного представителя, в ЦУС VPN осуществляется в день прибытия Оператора, или его полномочного представителя.

8.1.2. Изготовление сертификата открытого ключа Оператора ЦУС VPN посредством Web-интерфейса ЦУС VPN.

При изготовлении первого сертификата открытого ключа посредством Web-интерфейса Оператор ЦУС VPN должен заполнить регистрационную форму.

Ответственность за правильность указания идентификационных данных полностью возлагается на Оператора ЦУС VPN. После заполнения указанной регистрационной формы Оператор ЦУС VPN получает Маркер временного доступа.

На Оператора ЦУС VPN должна быть оформлена доверенность, уполномочивающая его выступать в роли Оператора ЦУС VPN и совершать действия, определенные положениями настоящего Регламента для Оператора ЦУС VPN. Указанная доверенность оформляется по форме Приложения № 2 настоящего Регламента, после чего Оператор ЦУС VPN сканирует этот бумажный документ и файл (файлы), являющийся результатом сканирования, направляет в ЦУС VPN по электронной почте. Оригинал доверенности Оператора ЦУС VPN направляется в ЦУС VPN посредством почтовой или курьерской связи.

При изготовлении второго и последующих сертификатов открытых ключей Оператор может получить возможность изготовления сертификата открытого ключа по Маркеру временного доступа или из Личного кабинета на ЦУС VPN. В том случае, если доступ Оператора ЦУС VPN в Личный кабинет невозможен, ЦУС VPN по запросу Оператора ЦУС VPN предоставляет Маркер временного доступа. Способ предоставления Маркера временного доступа определяется Оператором ЦУС VPN по согласованию с ЦУС VPN.

При изготовлении второго и последующих сертификатов Оператора ЦУС VPN должен располагать действующей доверенностью, уполномочивающей его выступать в роли Оператора ЦУС VPN и совершать действия, определенные положениями настоящего Регламента для Оператора ЦУС VPN, оформленной по форме Приложения № 2 настоящего Регламента.

С помощью Web-интерфейса ЦУС VPN (по Маркеру временного доступа или из Личного кабинета) Оператор формирует закрытый ключ и запрос на изготовление сертификата открытого ключа в электронной форме. После этого Оператор ЦУС VPN распечатывает заявление на изготовление сертификата открытого ключа по форме Приложения № 4 и надлежащим образом оформляет его. Наличие собственноручной подписи Оператора ЦУС VPN на заявлении на изготовление сертификата свидетельствует о том, что Оператор ЦУС VPN является владельцем закрытого ключа и соответствующего ему открытого ключа, который содержится в заявлении на изготовление сертификата.

После оформления заявления на изготовление сертификата Оператор ЦУС VPN обеспечивает сканирование этого бумажного документа и файл (файлы), являющийся результатом сканирования, направляет в ЦУС VPN по электронной почте. Оригинал заявления на изготовление сертификата открытого ключа направляется в ЦУС VPN посредством почтовой или курьерской связи.

После поступления сканированного заявления в ЦУС VPN Администратор ЦУС VPN производит сравнение информации, указанной в заявлении на изготовление сертификата с информацией, указанной в запросе на изготовление сертификата, поданном в электронной форме, и принимает решение об изготовлении сертификата открытого ключа Оператора ЦУС VPN.

В случае отказа в изготовлении сертификата открытого ключа Оператор ЦУС VPN уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Администратор ЦУС VPN изготавливает сертификат открытого ключа Оператора ЦУС VPN.

Изготовление сертификата и уведомление Оператора ЦУС VPN об этом должны быть осуществлены не позднее 3-х (Трёх) рабочих дней следующих за рабочим днем, в течение которого было получено Администратором ЦУС VPN сканированное заявление на изготовление сертификата открытого ключа. Уведомление Оператора ЦУС VPN осуществляется ЦУС VPN по электронной почте.

После получения уведомления об изготовлении сертификата Оператор ЦУС VPN с помощью Web-интерфейса ЦУС VPN (по Маркеру временного доступа или из

Личного кабинета, в зависимости от того, как Оператор ЦУС VPN формировал закрытый ключ и запрос на изготовление сертификата открытого ключа) получает сертификат открытого ключа.

8.2. Аннулирование (отзыв) сертификата открытого ключа Оператора ЦУС VPN

ЦУС VPN аннулирует сертификат открытого ключа Оператора ЦУС VPN в следующих случаях:

- в случае расторжения Договора на предоставление услуг ЦУС VPN;
- по заявлению Оператора ЦУС VPN;
- по заявлению на отзыв доверенности Оператора ЦУС VPN;
- по истечении срока его действия;
- по истечении срока, на который действие сертификата было приостановлено;
- при компрометации закрытого ключа Уполномоченного лица ЦУС VPN.

В случае расторжения Договора на предоставление услуг ЦУС VPN, истечения срока, на который действие сертификата открытого ключа было приостановлено, отзыва сертификата Оператора по его заявлению, отзыва сертификата по заявлению на отзыв доверенности ЦУС VPN должен официально уведомить Оператора и всех лиц, зарегистрированных в ЦУС VPN, об аннулировании (отзыве) сертификата не позднее одного рабочего дня с момента наступления описанного события.

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

Информация о размещении списка отозванных сертификатов заносится в изданные ЦУС VPN сертификаты открытых ключей в расширение `CRL Distribution Point` сертификата открытого ключа.

В случае аннулирования сертификата открытого ключа Оператора ЦУС VPN по истечении срока его действия временем аннулирования сертификата открытого ключа Оператора ЦУС VPN признается время, хранящееся в поле `notAfter` поля `Validity` сертификата открытого ключа. В данном случае информация об аннулированном сертификате открытого ключа Оператора ЦУС VPN в список отозванных сертификатов не заносится.

В случае компрометации закрытого ключа Уполномоченного лица ЦУС VPN временем аннулирования сертификата открытого ключа Оператора ЦУС VPN признается время компрометации закрытого ключа ЦУС VPN, фиксирующееся в реестре ЦУС VPN. В случае компрометации закрытого ключа Уполномоченного лица ЦУС VPN информация о сертификате открытого ключа Оператора ЦУС VPN в список отозванных сертификатов не заносится.

8.2.1. Аннулирование (отзыв) сертификата открытого ключа Оператора ЦУС VPN по заявлению его владельца

Заявление на аннулирование (отзыв) сертификата открытого ключа должно быть оформлено по форме Приложения № 5. После оформления заявления на аннулирование (отзыв) сертификата Оператор ЦУС VPN обеспечивает сканирование этого бумажного документа и файл (файлы), являющийся результатом сканирования, направляет в ЦУС VPN по электронной почте. Оригинал заявления на

аннулирование (отзыв) сертификата открытого ключа направляется в ЦУС VPN посредством почтовой или курьерской связи.

После поступления сканированного заявления в ЦУС VPN Администратор ЦУС VPN 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 ЦУС VPN.

В случае отказа в отзыве сертификата открытого ключа ЦУС VPN уведомляет об этом Оператора ЦУС VPN.

При принятии положительного решения Администратор ЦУС VPN отзывает сертификат открытого ключа Оператора ЦУС VPN.

8.2.2. Аннулирование (отзыв) сертификата открытого ключа Оператора ЦУС VPN по заявлению на отзыв доверенности

Уполномоченная Организация (Оператор предоставления услуг ЦУС VPN) вправе отозвать сертификаты открытых ключей своих полномочных представителей – Операторов ЦУС VPN, путем подачи заявления на отзыв доверенности Оператора ЦУС VPN.

Форма заявления на отзыв доверенности приведена в Приложении № 6 к настоящему Регламенту. После оформления заявления на отзыв доверенности Уполномоченная Организация обеспечивает сканирование этого бумажного документа и файл (файлы), являющийся результатом сканирования, направляет в ЦУС VPN по электронной почте. Оригинал заявления на отзыв доверенности направляется в ЦУС VPN посредством почтовой или курьерской связи.

После получения ЦУС VPN сканированного заявления на отзыв доверенности Администратор ЦУС VPN осуществляет его 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 ЦУС VPN.

В случае отказа в отзыве сертификата открытого ключа Оператора ЦУС VPN уведомляет об этом Уполномоченную Организацию с указанием обоснованных причин отказа.

При принятии положительного решения Администратор ЦУС VPN отзывает сертификат открытого ключа Оператора ЦУС VPN.

8.3. Приостановление действия сертификата открытого ключа Оператора ЦУС VPN

ЦУС VPN приостанавливает действие сертификата открытого ключа Оператора ЦУС VPN в следующих случаях:

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

Действие сертификата открытого ключа Оператора ЦУС VPN приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата открытого ключа составляет 15 (Пятнадцать) дней.

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

Официальным уведомлением о факте приостановления действия сертификата открытого ключа 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 открытого ключа признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные ЦУС VPN сертификаты открытых ключей в расширение CRL Distribution Point сертификата открытого ключа.

8.3.1. Приостановление действия сертификата открытого ключа Оператора ЦУС VPN по заявлению его владельца

Заявление на приостановление действия сертификата открытого ключа должно быть оформлено по форме Приложения № 7. После оформления заявления на приостановление действия сертификата Оператор ЦУС VPN обеспечивает сканирование этого бумажного документа и файл (файлы), являющийся результатом сканирования, направляет в ЦУС VPN по электронной почте. Оригинал заявления на приостановление действия сертификата открытого ключа направляется в ЦУС VPN посредством почтовой или курьерской связи.

После поступления сканированного заявления в ЦУС VPN Администратор ЦУС VPN осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято ЦУС VPN.

В случае отказа в приостановлении действия сертификата открытого ключа ЦУС VPN уведомляет об этом Оператора ЦУС VPN.

При принятии положительного решения Администратор ЦУС VPN приостанавливает действие сертификата открытого ключа Оператора ЦУС VPN.

8.3.2. Приостановление действия сертификата открытого ключа Оператора ЦУС VPN по заявлению в устной форме

Приостановление действия сертификата открытого ключа по заявлению Оператора ЦУС VPN в устной форме осуществляется исключительно при компрометации закрытого ключа или подозрении в компрометации закрытого ключа Оператора ЦУС VPN.

Заявление подается в ЦУС VPN по телефону.

Оператор ЦУС VPN должен сообщить Администратору ЦУС VPN следующую информацию:

- идентификационные данные, содержащиеся в сертификате открытого ключа, действие которого необходимо приостановить;
- серийный номер сертификата открытого ключа, действие которого требуется приостановить.

После принятия заявления Администратор ЦУС VPN принимает решение о приостановлении действия сертификата открытого ключа, которое должно быть осуществлено в течение рабочего дня поступления данного заявления.

В случае отказа в приостановлении действия сертификата открытого ключа Оператор ЦУС VPN уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, Администратор ЦУС VPN приостанавливает действие сертификата открытого ключа до окончания срока действия закрытого ключа Оператора ЦУС VPN.

Не позднее 5 (Пяти) рабочих дней с момента приостановления действия сертификата открытого ключа Оператор ЦУС VPN должен предоставить в ЦУС VPN заявление на аннулирование (отзыв) сертификата открытого ключа (в том случае, если факт компрометации закрытого ключа подтвердился), либо заявление на возобновление действия сертификата открытого ключа (в том случае, если компрометации закрытого ключа не было).

8.3.3. Приостановление действия сертификата открытого ключа по решению ЦУС VPN

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

После приостановления действия сертификата открытого ключа Администратор ЦУС VPN сообщает Оператору ЦУС VPN о наступлении события, повлекшего приостановление действия сертификата, и уведомляет его о том, что действие сертификата Оператора ЦУС VPN приостановлено.

8.4. Возобновление действия сертификата открытого ключа Оператора ЦУС VPN

ЦУС VPN возобновляет действие сертификата открытого ключа Оператора ЦУС VPN только в том случае, если действие данного сертификата открытого ключа приостановлено. ЦУС VPN возобновляет действие сертификата открытого ключа Оператора ЦУС VPN только по заявлению Оператора ЦУС VPN.

Официальным уведомлением о факте возобновления действия сертификата открытого ключа 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 открытого ключа признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные ЦУС VPN сертификаты открытых ключей в расширение CRL Distribution Point.

8.4.1. Возобновление действия сертификата открытого ключа по заявлению Оператора ЦУС VPN

Заявление на возобновление действия сертификата открытого ключа Оператора ЦУС VPN должно быть оформлено по форме Приложения № 8. После оформления заявления на возобновление действия сертификата Оператор ЦУС VPN обеспечивает сканирование этого бумажного документа и файл (файлы), являющийся результатом сканирования, направляет в ЦУС VPN по электронной почте. Оригинал заявления на возобновление действия сертификата открытого ключа направляется в ЦУС VPN посредством почтовой или курьерской связи.

После поступления сканированного заявления в ЦУС VPN Администратор ЦУС VPN осуществляет его рассмотрение и обработку. Обработка заявления на возобновление действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято ЦУС VPN.

В случае отказа в возобновлении действия сертификата открытого ключа ЦУС VPN уведомляет об этом Оператора ЦУС VPN.

При принятии положительного решения Администратор ЦУС VPN возобновляет действие сертификата открытого ключа Оператора ЦУС VPN.

8.5. Прочие условия

8.5.1. Стороны признают равную юридическую силу собственноручной подписи, выполненной на указанных в Разделе 8 документах, и факсимильной подписи, воспроизведенной в сканированных документах.

8.5.2. Если указанные в Разделе 8 документы должны быть заверены печатью, то Стороны признают равную юридическую силу указанных в Разделе 8 документов, заверенных печатью, и сканированных документов, содержащих факсимильное воспроизведение подписи.

8.6. Изготовление и управление сертификатами открытых ключей Пользователей ЦУС VPN

Принятие решений по изготовлению и управлению сертификатами открытых ключей Пользователей ЦУС VPN производится Оператором ЦУС VPN и осуществляется в соответствии с порядком, установленным Уполномоченной Организацией (Оператором услуг ЦУС VPN).

ЦУС VPN выполняет действия по изготовлению сертификатов открытых ключей, отзыву сертификатов открытых ключей, приостановлению и возобновлению действий сертификатов открытых ключей на основании заявлений в электронной форме, подписанных усиленной электронной подписью Оператором ЦУС VPN, и направляемых Оператором ЦУС VPN с использованием АРМ администратора ЦР. В качестве средства электронной подписи используется СКЗИ «КриптоПро CSP».

Указанные заявления в электронной форме представляют собой криптографические сообщения формата CMS. В качестве подписанных данных используются запросы на изготовление сертификата, запросы на отзыв сертификата, запросы на приостановление действия сертификата, запросы на возобновление действия сертификата, а электронная подпись для указанных данных формируется на закрытом ключе (ключе электронной подписи) Оператора ЦУС VPN, соответствующем сертификату открытого ключа (сертификату ключа проверки электронной подписи) Оператора ЦУС VPN.

Запрос на изготовление сертификата представляет собой сообщение формата PKCS#10.

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

- CertificateSerialNumber - серийный номер отзываемого сертификата открытого ключа;
- ReasonCode - код причины отзыва из следующего перечня допустимых значений: "0" - Не указана; "1" - Компрометация ключа; "2"- Компрометация ключа издателя; "3" - Изменение принадлежности; "4" - Сертификат заменен; "5" - Прекращение работы;
- SomeComment - текстовое значение комментария владельца сертификата или Оператора ЦУС VPN.

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

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

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

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

Выполнение действий по изготовлению и управлению сертификатов Пользователей ЦУС VPN осуществляется ЦУС VPN по заявлениям Оператора ЦУС VPN, направляемым в электронной форме, при одновременном выполнении следующих условий:

- Подтверждена подлинность электронной подписи Оператора ЦУС VPN в направленном заявлении;
- Сертификат открытого ключа Оператора ЦУС VPN и соответствующий ему закрытый ключ на момент получения заявления ЦУС VPN действительны;
- Сертификат открытого ключа Оператора ЦУС VPN содержит в расширении Extended Key Usage объектный идентификатор - 1.2.643.2.2.34.5, соответствующий области использования сертификата и ключа – Оператор Центра Регистрации.

9. Управление ключами и сертификатами уполномоченного лица ЦУС VPN

9.1. Плановая смена ключей уполномоченного лица ЦУС VPN

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица ЦУС VPN выполняется в период действия закрытого ключа уполномоченного лица ЦУС VPN.

Старый закрытый ключ уполномоченного лица ЦУС VPN используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных ЦУС VPN в период действия старого закрытого ключа уполномоченного лица ЦУС VPN.

9.2. Компрометация ключевых документов уполномоченного лица ЦУС VPN, внеплановая смена ключей уполномоченного лица ЦУС VPN.

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

После аннулирования сертификата уполномоченного лица ЦУС VPN выполняется процедура внеплановой смены ключей уполномоченного лица ЦУС

VPN. Процедура внеплановой смены ключей уполномоченного лица ЦУС VPN соответствует процедуре плановой смены ключей уполномоченного лица ЦУС VPN.

Все действовавшие на момент компрометации закрытого ключа уполномоченного лица ЦУС VPN сертификаты открытых ключей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

10. Конфиденциальность информации, персональные данные

10.1. Типы конфиденциальной информации

Закрытый ключ, соответствующий сертификату открытого ключа является конфиденциальной информацией лица, зарегистрированного в ЦУС VPN. ЦУС VPN не осуществляет хранение закрытых ключей пользователей ЦУС VPN.

Персональная и корпоративная информация о лицах, зарегистрированных в ЦУС VPN, не подлежащая непосредственной рассылке в качестве части сертификата открытого ключа, считается конфиденциальной.

ЦУС VPN имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях установленных законодательством Российской Федерации.

10.2. Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Открытая информация может публиковаться по решению ЦУС VPN. Место, способ и время публикации открытой информации определяется ЦУС VPN.

Информация, включаемая в сертификаты открытых ключей и списки отозванных сертификатов, издаваемые ЦУС VPN, не считается конфиденциальной.

Персональные данные, включаемые в сертификаты открытых ключей, издаваемые ЦУС VPN, относятся к общедоступным персональным данным.

11. Структура сертификатов открытых ключей и списков отозванных сертификатов, сроки действия ключевых документов

11.1. Структура сертификатов открытых ключей и списков отозванных сертификатов

Структура сертификатов открытых ключей и списков отозванных сертификатов, издаваемых ЦУС VPN, приведена в Приложении №9 настоящего Регламента.

11.2. Сроки действия ключевых документов

11.2.1. Сроки действия ключевых документов уполномоченного лица ЦУС VPN

Срок действия закрытого ключа уполномоченного лица ЦУС VPN составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности ЦУС VPN, и для средства криптографической защиты информации, с использованием которых данный закрытый ключ был сформирован.

Начало периода действия закрытого ключа уполномоченного лица ЦУС VPN исчисляется с времени начала действия соответствующего сертификата открытого ключа.

Срок действия сертификата открытого ключа уполномоченного лица ЦУС VPN не превышает 30 (Тридцать) лет. Время начала периода действия сертификата

открытого ключа уполномоченного лица ЦУС VPN и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity» соответственно.

11.2.2. Сроки действия ключевых документов Оператора и Пользователя ЦУС VPN.

Срок действия закрытого ключа Оператора и Пользователя ЦУС VPN составляет 1 (Один) год.

Начало периода действия закрытого ключа Оператора и Пользователя ЦУС VPN исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа.

Срок действия сертификата открытого ключа Оператора и Пользователя ЦУС VPN составляет 1 (Один) год. Время начала периода действия сертификата открытого ключа Оператора и Пользователя ЦУС VPN и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity» соответственно.

12. Дополнительные положения

12.1. Хранение изданных сертификатов открытых ключей в ЦУС VPN

Срок хранения сертификата открытого ключа, изданного в ЦУС VPN осуществляется в течение всего периода его действия и 5 (Пяти) лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты открытых ключей переводятся в режим архивного хранения.

12.2. Прекращение оказания услуг ЦУС VPN

12.2.1. В случае расторжения договора на оказание услуг ЦУС VPN сертификаты открытых ключей, решение по изготовлению которых было принято Уполномоченной Организацией (Оператором предоставления услуг ЦУС VPN) могут быть аннулированы (отозваны) по решению ЦУС VPN.

12.3. Форс-мажор

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

12.3.2. 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.

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

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

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

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

13. Список приложений

- 13.1. Приложение №1. Форма заявления на изготовление сертификата открытого ключа Оператора ЦУС VPN (при изготовлении сертификата открытого ключа при личном прибытии Оператора, либо его полномочного представителя, в ЦУС VPN).
- 13.2. Приложение №2. Форма доверенности Оператора ЦУС VPN
- 13.3. Приложение №3. Форма доверенности на получение закрытых ключей и сертификата открытого ключа за Оператора ЦУС VPN (при изготовлении сертификата открытого ключа при прибытии полномочного представителя Оператора ЦУС VPN в ЦУС VPN).
- 13.4. Приложение №4. Форма заявления на изготовление сертификата открытого ключа Оператора ЦУС VPN (при изготовлении сертификата открытого ключа посредством Web-интерфейса ЦУС VPN).
- 13.5. Приложение №5. Форма заявления на аннулирование (отзыв) сертификата открытого ключа Оператора ЦУС VPN.
- 13.6. Приложение №6. Форма заявления на отзыв доверенности Оператора ЦУС VPN.
- 13.7. Приложение №7. Форма заявления на приостановление действия сертификата открытого ключа Оператора ЦУС VPN.
- 13.8. Приложение №8. Форма заявления на возобновление действия сертификата открытого ключа Пользователя ЦУС VPN.
- 13.9. Приложение №9. Структура сертификатов открытых ключей и списков отозванных сертификатов, издаваемых ЦУС VPN.

Приложение №1
к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма заявления на изготовление сертификата открытого ключа
Оператора ЦУС VPN при личном прибытии Оператора,
либо его полномочного представителя, в ЦУС VPN)

Заявление на изготовление сертификата открытого ключа
Оператора ЦУС VPN

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

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

действующего на основании _____

Просит сформировать закрытый ключ, записать сформированный закрытый ключ на предоставленный ключевой носитель и изготовить сертификат открытого ключа полномочного представителя – Оператора ЦУС VPN

_____ (фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными:

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

Оператор ЦУС VPN

« ____ » _____ 20__ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

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

Доверенность

г. _____ « ____ » _____ 20__ г.

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____ (фамилия, имя, отчество)

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

выступать в роли Оператора ЦУС VPN и осуществлять действия в рамках Регламента ЦУС VPN, установленных для Оператора ЦУС VPN.

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

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

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

подтверждаю.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №3

к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма доверенности на получение закрытого ключа
и сертификата открытого ключа за Оператора ЦУС VPN)

Доверенность

г. _____ « ____ » _____ 20__ г.

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____ (фамилия, имя, отчество)

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

1. Предоставить в ООО «КРИПТО-ПРО» (ЦУС VPN) необходимые документы, определенные Регламентом ЦУС VPN для изготовления сертификата открытого ключа Оператора ЦУС VPN;
2. Получить сформированный закрытый ключ и изданный сертификат открытого ключа Оператора ЦУС VPN:

_____ (фамилия, имя, отчество)

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

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

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

подтверждаю.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №4

к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма заявления на изготовление сертификата открытого ключа
Оператора ЦУС VPN посредством Web-интерфейса ЦУС VPN)

Заявление на изготовление сертификата открытого ключа
Оператора ЦУС VPN

Прошу изготовить в ЦУС VPN сертификат открытого ключа
в соответствии с указанными данными:

Сведения о запросе на сертификат:

Этот запрос:

Кем выпущен:

User1

Версия: 1 (0x0)

Субъект запроса на сертификат: CN = User1

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

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(1.2.643.2.2.34.5) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

3. Атрибут 1.3.6.1.4.1.311.13.2.2

Название: CSP заявки

Сведения о провайдере

Назначение ключа : ОБМЕН

Название провайдера : Crypto-Pro GOST R 34.10-2001 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:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-94

Параметры: 0500

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

Подпись владельца закрытого ключа – Оператора ЦУС VPN: _____/_____
" __ " _____ 20__ г.

Подпись руководителя организации: _____/_____
" __ " _____ 20__ г.

М.П.

Приложение №5
к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма заявления на аннулирование (отзыв) сертификата
открытого ключа Оператора ЦУС VPN)

Заявление на аннулирование (отзыв) сертификата открытого ключа
Оператора ЦУС VPN

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

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Просит аннулировать (отозвать) сертификат открытого ключа своего полномочного представителя – Оператора ЦУС VPN: _____
(фамилия, имя, отчество)

содержащий следующие данные:

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

Оператор ЦУС VPN

«_____» _____ 20____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №6

к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма заявления на отзыв доверенности Оператора ЦУС VPN)

Заявление на отзыв доверенности Оператора ЦУС VPN

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

Заявляет, что отзывает Доверенность № _____ от « _____ » _____ 20__ года,
выданную для представления в ЦУС VPN своему полномочному представителю –
Оператору ЦУС VPN _____

(фамилия, имя, отчество)

и просит аннулировать (отозвать) сертификаты открытых ключей, содержащие
область использования - Оператор Центра Регистрации (1.2.643.2.2.34.5), владельцем
которых является данный Оператор ЦУС VPN.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №7
к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма заявления на приостановление действия сертификата
открытого ключа Оператора ЦУС VPN)

Заявление на приостановление действия сертификата открытого ключа
Оператора ЦУС VPN

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

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие сертификата открытого ключа своего полномочного представителя – Оператора ЦУС VPN:

_____ (фамилия, имя, отчество)

содержащего следующие данные:

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

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

Оператор ЦУС VPN

_____ 20__ г.
« ____ » _____

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Приложение №8
к Регламенту ЦУС VPN (Схема обслуживания: распределенная с оператором)
(Форма заявления на возобновление действия сертификата
открытого ключа Оператора ЦУС VPN)

Заявление на возобновление действия сертификата открытого ключа
Оператора ЦУС VPN

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

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата открытого ключа своего полномочного представителя – Оператора ЦУС VPN:

_____ (фамилия, имя, отчество)

содержащего следующие данные:

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

Оператор ЦУС VPN

_____ г.
« ____ » _____ 20 ____ г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Структура сертификатов открытых ключей и списков отозванных сертификатов,
издаваемых ЦУС VPN

Структура сертификата открытого ключа уполномоченного лица ЦУС VPN:

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	CN = CryptoPro VPN CA O = Организация = Crypto-Pro Ltd. L = Город = Moscow C = Страна/Регион = RU E = Электронная почта = vpnca@cryptopro.ru
Validity	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс UTC Действителен по: дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CN = CryptoPro VPN CA O = Организация = Crypto-Pro Ltd. L = Город = Moscow C = Страна/Регион = RU E = Электронная почта = vpnca@cryptopro.ru (Поля Issuer и Subject идентичны)
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	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage	Использование ключа	Цифровая подпись, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа уполномоченного лица ЦУС VPN, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) =ЦС Path Length Constraint (Ограничение на длину пути –ограничивает количество уровней иерархии при создании подчиненных центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата	Версия сертификата уполномоченного лица ЦУС VPN

Структура списка отозванных сертификатов ЦУС VPN

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = CryptoPro VPN CA O = Организация = Crypto-Pro Ltd. L = Город = Moscow C = Страна/Регион = RU E = Электронная почта = vpnca@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 <ol style="list-style-type: none"> 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) <ul style="list-style-type: none"> "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП 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 ЦУС VPN, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица ЦУС VPN
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС

Структура сертификата открытого ключа Оператора и Пользователя ЦУС VPN

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	CN = CryptoPro VPN CA O = Организация = Crypto-Pro Ltd. L = Город = Moscow C = Страна/Регион = RU E = Электронная почта = vpnca@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	CN = ФИО или Псевдоним O = Организация OU = Подразделение L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280, RFC 5280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage	Использование ключа	Неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов Для Оператора ЦУС VPN: Оператор Центра Регистрации - (1.2.643.2.2.34.5) Проверка подлинности клиента - (1.3.6.1.5.5.7.3.2)
Application Policy	Политика применения	Набор областей использования ключей и сертификатов
Certificate Policies	Политики сертификатов	Набор областей использования ключей и сертификатов
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица ЦУС VPN, 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
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280, RFC 5280