Утвержден
Приказом ООО «КРИПТО-ПРО» №21/02-01
от «15» февраля 2021 г.

# РЕГЛАМЕНТ

Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)

Редакция № 2

г. Москва
2021

# 1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дельнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва (Свидетельство о внесении записи в единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 01 июля 2002 года серия 77 №007360250 от 29.01.2003 г.).

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании Свидетельства об аккредитации удостоверяющего центра № 743 от 28.07.2017, выданного Министерством связи и массовых коммуникаций Российской Федерации, и на основании следующей лицензии:

**Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 12936 Н от 11 июня 2013 г. на осуществление** разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

**Реквизиты ООО «КРИПТО-ПРО»:**

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

**Юридический адрес:** 105037, г. Москва, Измайловский проезд, д. 10, корп. 2, эт. 1, пом. IV

**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):

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

**ИНН/КПП:** 7717107991/771901001

**ОГРН:** 1037700085444

**Контактные телефоны, факс, адрес электронной почты:**

тел./факс (495) 995-48-20; e-mail: qca@cryptopro.ru, info@cryptopro.ru

## 2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные в Федеральном законе от 6 апреля 2011 года №63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи») и Договором, заключаемым между *Удостоверяющим центром и Уполномоченной организацией*, а также термины и определения их дополняющие и конкретизирующие, а именно:

*Администратор Удостоверяющего центра* – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по обеспечению создания ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, прекращение, приостановление и возобновление действия) сертификатами ключей проверки электронной подписи Операторов Удостоверяющего центра, приостановлением действия сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром заверять копии сертификатов ключей проверки электронной подписи Операторов Удостоверяющего центра на бумажном носителе.

*Веб-интерфейс, предоставляемый Удостоверяющим центром* – интерфейс взаимодействия Пользователя Удостоверяющего центра и Оператора Удостоверяющего центра с Удостоверяющим центром и Сервисом электронной подписи, предназначенный для управления сертификатами ключей проверки электронной подписи и получения доступа к функциям электронной подписи, реализованный в виде набора веб-страниц и размещенный на веб-узле Удостоверяющего центра.

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

*Заявитель* – юридическое лицо, индивидуальный предприниматель, иной хозяйствующий субъект, физическое лицо, обращающееся с соответствующим заявлением в Удостоверяющий центр на создание и выдачу сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

*Информационная система Уполномоченной организации* - обобщенное понятие корпоративной информационной системы Уполномоченной организации, которая подключается к Сервису электронной подписи для получения доступа к функциям электронной подписи и управления сертификатами ключей проверки электронной подписи.

*Ключ электронной подписи* - уникальная последовательность символов, предназначенная для создания электронной подписи.

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

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

*Ключ электронной подписи Удостоверяющего центра* – ключ электронной подписи, использующийся Удостоверяющим центром для создания сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

*Ключ проверки электронной подписи* – уникальная последовательность символов, однозначно связанная с ключом электронной подписи, предназначенная для проверки подлинности электронной подписи.

*Копия сертификата ключа проверки электронной подписи* – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра, либо подписанный Оператором Удостоверяющего центра и заверенный печатью Уполномоченной

организации. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

*Многофакторная аутентификация* - процедура проверки подлинности Пользователя Удостоверяющего центра при осуществлении доступа с использованием двух и более уникальных характеристик, известных или присущих только Пользователю Удостоверяющего центра (факторов аутентификации). При управлении доступом к Сервису электронной подписи для первичной аутентификации Пользователя Удостоверяющего Центра используется постоянно действующий пароль, самостоятельно определяемый Пользователем Удостоверяющего центра, для вторичной аутентификации – ключ аутентификации в мобильном приложении myDSS из состава ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» версии 2.0» на устройствах пользователей; одноразовый пароль, формируемый Сервисом электронной подписи и высылаемый Пользователю Удостоверяющего центра в информационном сообщении на номер мобильного телефона, указанный Пользователем Удостоверяющего центра при регистрации, или OTP-токеном, выдаваемый Оператором УЦ по заявлению Пользователя Удостоверяющего центра. Уполномоченная организация вправе использовать дополнительные факторы аутентификации для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи совместно с собственным Сторонним центром идентификации. Уполномоченная организация самостоятельно осуществляет выбор используемых средств аутентификации пользователей в соответствии с условиями сертификации ПАК «КриптоПро DSS» на соответствие к требованиям электронной подписи согласно документу «ЖТЯИ.00096-02 30 01. КриптоПро HSM. Формуляр».

*Мобильное приложение myDSS* – компонент ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» версии 2.0», устанавливаемый на мобильном устройстве Пользователей УЦ.

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

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

*Оператор Стороннего центра идентификации (Оператор СЦИ)* – Оператор УЦ, зарегистрированный в Стороннем центре идентификации Уполномоченной организации, действующий от имени Уполномоченной организации по обеспечению создания и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, зарегистрированных в том же Стороннем центре идентификации Уполномоченной организации.

*Оператор Сервиса электронной подписи (Оператор СЭП), Оператор Удостоверяющего центра (Оператор УЦ)* — физическое лицо, действующее от имени Уполномоченной Организации, совершающее действия по регистрации пользователей в Сервисе электронной подписи и управлению параметрами доступа пользователей к Сервису электронной подписи, а также по принятию решений о создании, выдаче (вручении) и управлении квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра для использования в информационной системе Уполномоченной организации.

*Пользователь Удостоверяющего центра (Пользователь УЦ)* – физическое лицо, являющееся владельцем квалифицированного сертификата ключа проверки электронной

подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец сертификата ключа проверки электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица, присоединившееся к Регламенту Уполномоченной организации.

*Прикладной интерфейс, предоставляемый Удостоверяющим центром (API)* – интерфейс подключения Информационных систем Уполномоченной организации к Удостоверяющему центру по линиям связи для получения доступа к функциям электронной подписи, управления сертификатами ключей проверки электронной подписи, реализованный в соответствии с руководством разработчика на программное обеспечение «КриптоПро DSS» и защищенный с использованием средств криптографической защиты информации, совместимых со средствами Удостоверяющего центра.

*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.

*Регламент Уполномоченной организации* – локальный нормативный документ Уполномоченной организации, определяющий условия предоставления и правила пользования услугами Удостоверяющего центра по созданию, управлению и выдаче сертификатов ключей проверки электронной подписи, получения доступа и пользования Сервисом электронной подписи для Пользователей Удостоверяющего центра.

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

- реестр заявлений на регистрацию пользователей в Удостоверяющем центре;
- реестр зарегистрированных Пользователей Удостоверяющего центра;
- реестр заявлений на создание сертификатов ключей проверки электронной подписи;
- реестр заявлений на прекращение действия (аннулирование) сертификатов ключей проверки электронной подписи;
- реестр заявлений на приостановление/возобновление действия сертификатов ключей проверки электронной подписи;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;
- реестр сертификатов ключей проверки электронной подписи;
- реестр изготовленных списков отозванных сертификатов ключей проверки электронной подписи.

*Сервис электронной подписи (СЭП)* - комплекс организационных, технических и программных средств Удостоверяющего центра, обеспечивающих для Пользователей Удостоверяющего центра удаленную реализацию функций централизованного создания и хранения ключей электронной подписи, создания и проверки усиленной квалифицированной электронной подписи электронных документов, аутентификации владельцев сертификатов ключей проверки электронной подписи при осуществлении доступа к СЭП и выполнении операций с использованием принадлежащих им ключей электронной подписи. Доступ Пользователей УЦ к СЭП осуществляется посредством Веб-интерфейса, предоставляемого Удостоверяющим центром, или подключенной к СЭП Информационной системы Уполномоченной организации.

*Сертификат ключа проверки электронной подписи (Квалифицированный сертификат ключа проверки электронной подписи, Сертификат)* - электронный документ, выданный Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;

- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие и действие его не приостановлено.

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

*Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра (Сертификат Пользователя УЦ)* - сертификат ключа проверки электронной подписи, соответствующий которому ключ электронной подписи создан и хранится с использованием СЭП.

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

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

*Служба актуальных статусов сертификатов* – сервис Удостоверяющего центра (построенный на базе протокола OCSP – Online Certificate Status Protocol), с использованием которого подписываются электронной подписью и предоставляются Пользователям УЦ электронные метки, содержащие информацию о статусе сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

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

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

*Средство криптографической защиты информации (СКЗИ)* – программа для ЭВМ или программно-аппаратный комплекс, осуществляющий шифрование данных в целях обеспечения безопасности передачи информации.

*Средство электронной подписи* – средство криптографической защиты информации в соответствии с положениями настоящего Регламента, используемое для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и (или) ключа проверки электронной подписи.

*Сторонний центр идентификации* – система аутентификации Уполномоченной организации, подключаемая к Сервису электронной подписи по протоколу SAML в соответствии с документацией на программное обеспечение «КриптоПро DSS» и используемая Уполномоченной организацией для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи.

*Тестовый сертификат* – временный неквалифицированный сертификат ключа проверки электронной подписи, выданный тестовым Удостоверяющим центром, не имеющий

юридической силы и предназначенный исключительно для тестирования функциональности СЭП.

*Удостоверяющий центр* – ООО «КРИПТО-ПРО», осуществляющее выполнение целевых функций удостоверяющего центра по созданию, выдаче и управлению квалифицированными сертификатами ключей проверки электронной подписи в соответствии с Федеральным законом «Об электронной подписи», а также предоставляющее Сервис электронной подписи в целях обеспечения применения участниками Информационной Системы Уполномоченной организации усиленной квалифицированной электронной подписи.

*Уполномоченная организация* – юридическое лицо, заключившее с Удостоверяющим центром договор, наделяющий данное юридическое лицо полномочиями по принятию решений по созданию, управлению и обеспечению выдачи квалифицированных сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра и управлению доступом к Сервису электронной подписи.

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

*Электронная подпись (ЭП)* – усиленная квалифицированная электронная подпись, являющаяся информацией в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

*Электронный документ* – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

*Cryptographic Message Syntax (CMS)* – стандарт 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, GOSTR 34.11-94, GOSTR 34.10-94, and GOSTR 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

*Online Certificate Status Protocol (OCSP)* – протокол установления статуса сертификата ключа проверки электронной подписи, реализующий RFC2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».

*OTP-токен* – специализированное персональное устройство, реализующее в соответствии с RFC 6238 Time-based One Time Password Algorithmили RFC 4226 HMAC-Based One-Time Password Algorithm создание одноразовых паролей для аутентификации Пользователя Удостоверяющего центра при осуществлении доступа к СЭП и подтверждения использования принадлежащего Пользователю Удостоверяющего центра ключа электронной подписи.

*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 ключа проверки электронной подписи.

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

*Short Message Service (SMS-сообщение, информационное сообщение)* («служба коротких сообщений») — технология, позволяющая осуществлять приём и передачу коротких текстовых сообщений с помощью сотового (мобильного) телефона.

*SMS-шлюз* – служба рассылки информационных сообщений Уполномоченной Организации, подключаемая к Сервису электронной подписи в соответствии с документацией на программное обеспечение «КриптоПро DSS» и используемая Уполномоченной

организацией для отправки Пользователям Удостоверяющего центра одноразовых паролей и уведомлений о выполняемых в СЭП операциях.

Принятие УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ решения по изготовлению (созданию) квалифицированного сертификата ключа проверки электронной подписи – это действия Оператора Удостоверяющего центра, необходимые для формирования и отправки в Удостоверяющий центр заявок в электронной форме на создание сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, с помощью средств, предоставляемых Удостоверяющим центром, и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

Принятие УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ решения по управлению квалифицированным сертификатом ключа проверки электронной подписи – это действия Оператора Удостоверяющего центра, необходимые для формирования и отправки в Удостоверяющий центр заявок в форме, установленной настоящим Регламентом, на приостановление, прекращение, возобновление действия квалифицированного сертификата ключа проверки электронной подписи Пользователей Удостоверяющего центра

Принятие УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ решения по приостановлению действия квалифицированного сертификата ключа проверки электронной подписи – это действия Оператора Удостоверяющего центра, необходимые для формирования и отправки в Удостоверяющий центр заявок в форме, установленной настоящим Регламентом, на приостановление действия квалифицированного сертификата ключа проверки электронной подписи Пользователей Удостоверяющего центра.

Принятие УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ решения по прекращению действия квалифицированного сертификата ключа проверки электронной подписи – это действия Оператора Удостоверяющего центра, необходимые для формирования и отправки в Удостоверяющий центр заявок в форме, установленной настоящим Регламентом, на прекращение действия квалифицированного сертификата ключа проверки электронной подписи Пользователей Удостоверяющего центра.

Принятие УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ решения по возобновлению действия квалифицированного сертификата ключа проверки электронной подписи – это действия Оператора Удостоверяющего центра, необходимые для формирования и отправки в Удостоверяющий центр заявок в форме, установленной настоящим Регламентом, на возобновление действия квалифицированного сертификата ключа проверки электронной подписи Пользователей Удостоверяющего центра.

# 3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент Удостоверяющего центра ООО «КРИПТО-ПРО» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи (Схема обслуживания: распределенная с оператором СЭП), 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 Уполномоченная организация.

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

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 Регламента

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

3.3.2. Уведомление о внесении изменений в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений на сайте Удостоверяющего центра по адресу: http://q.cryptopro.ru/reglament/reglamentoperdss.pdf.

3.3.3. Все изменения, вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении одного месяца со дня размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра по адресу: http://q.cryptopro.ru/reglament/reglamentoperdss.pdf.

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

3.3.5. Любые изменения 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 в силу.

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

## 4. Предоставление информации

4.1. Удостоверяющий центр осуществляет свою деятельность в качестве аккредитованного удостоверяющего центра на основании решения Минкомсвязи России, являющегося федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. С информацией по аккредитации Удостоверяющего центра можно ознакомиться на официальном сайте Минкомсвязи России.

4.2. Удостоверяющий центр осуществляет свою деятельность в соответствии с лицензиями ФСБ России на право осуществления технического обслуживания шифровальных (криптографических) средств, распространения шифровальных (криптографических) средств, оказания услуг в области шифрования информации. С копиями указанных лицензий можно ознакомиться по следующему адресу в сети Интернет - http://www.cryptopro.ru/about/licenses.

4.3. Удостоверяющий центр вправе запросить, а Уполномоченная организация обязана предоставить Удостоверяющему центру следующие документы:

- выписку или нотариально заверенную копию выписки из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента запроса Удостоверяющего центра;
- нотариально заверенные копии учредительных документов Уполномоченной организации;
- нотариально заверенную копию свидетельства о внесении записи о юридическом лице в Единый государственный реестр юридических лиц;
- нотариально заверенную копию свидетельства о постановке на учет в налоговом органе;
- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность - для Оператора Удостоверяющего центр (либо нотариально заверенные копии этих документов);
- иные документы, установленные Регламентом Удостоверяющего центра, а также дополнительные документы по усмотрению Удостоверяющего центра.

4.4. Уполномоченная организация в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» поручает Удостоверяющему центру в лице его уполномоченных работников и иных лиц, привлекаемых Удостоверяющим центром, совершать с персональными данными, содержащимися в документах, представленных Уполномоченной организацией Удостоверяющему центру, а также в документах, которые будут представлены Уполномоченной организацией Удостоверяющему центру в соответствии с настоящим Регламентом, следующие действия (с использованием и без использования средств автоматизации): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), в том числе передача уполномоченным работникам Удостоверяющего центра, обезличивание, блокирование, удаление, уничтожение персональных данных (далее – «обработка») в целях принятия Удостоверяющим центром решения о возможности доступа к СЭП, в целях исполнения настоящего Регламента, реализации вытекающих из настоящего Регламента прав и обязанностей, а также в целях осуществления Удостоверяющим центром функций, возложенных законодательством Российской Федерации.

Уполномоченная организация подтверждает, что персональные данные, содержащиеся в представляемых Уполномоченной организацией Удостоверяющему центру документах, не являются тайной частной жизни, личной и/или семейной тайной субъектов персональных данных.

Уполномоченная организация поручает Удостоверяющему центру в лице указанных выше работников и иных лиц, ими привлекаемых, осуществлять обработку персональных данных с соблюдением принципов и правил обработки персональных данных, предусмотренных

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», и обеспечением безопасности персональных данных при их обработке, на безвозмездной основе.

Уполномоченная организация подтверждает, что ею получено письменное согласие субъектов персональных данных, чьи персональные данные содержатся в представленных Уполномоченной организацией Удостоверяющему центру документах, на обработку Удостоверяющим центром этих персональных данных по поручению Уполномоченной организации в указанных выше целях, а также гарантирует, что содержащие персональные данные документы будут представляться Уполномоченной организацией Удостоверяющему центру в соответствии с настоящим Регламентом с согласия субъектов персональных данных, чьи персональные данные содержатся в таких документах. Письменное согласие Оператора СЭП на обработку его персональных данных УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ оформляется в форме Заявления на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра (Приложение №1 к настоящему Регламенту). Письменное согласие Пользователя Удостоверяющего центра на обработку его персональных данных УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ оформляется в заявлении на создание сертификата ключа проверки ЭП Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», формат которого определяется Регламентом Уполномоченной организации. Уполномоченная организация несет все неблагоприятные последствия, связанные с неполучением Уполномоченной организацией таких согласий.

Уполномоченная организация подтверждает, что ею получено письменное согласие субъектов персональных данных, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых они являются, относятся к общедоступным персональным данным.

Требования к защите обрабатываемых персональных данных, в т.ч. необходимые правовые, организационные и технические меры по защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении персональных данных определяются Удостоверяющим центром самостоятельно с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

## 5. Права и обязанности сторон

5.1. Удостоверяющий центр обязан:

5.1.1. Предоставить Оператору Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

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

5.1.3. Использовать ключ электронной подписи Удостоверяющего центра только для подписи создаваемых им сертификатов ключей проверки электронной подписи Удостоверяющего центра и списков отозванных сертификатов ключей проверки электронной подписи.

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

5.1.5. Организовать свою работу по рабочим дням. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

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

5.1.7. Создать сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра по заявлению на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, оформляемом по форме Приложения №1 к настоящему Регламенту, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.8. Предоставить аутентифицированным Пользователям Удостоверяющего центра, получившим сертификат ключа проверки электронной подписи в соответствии с Регламентом Уполномоченной организации, доступ к СЭП и обеспечить круглосуточное функционирование СЭП в режиме 24x7. Восстановить функционирование СЭП в течение 1 (одного) часа рабочего времени в случае проведения плановых регламентных работ или возникновения внештатных ситуаций. Доступные Пользователям функциональные возможности СЭП приведены в Приложении № 12 к настоящему Регламенту.

5.1.9. Использовать в составе СЭП сертифицированные средства криптографической защиты информации и электронной подписи для создания и хранения ключей электронной подписи Пользователей Удостоверяющего центра.

5.1.10. Принять меры по защите ключей электронной подписи Пользователей Удостоверяющего центра от несанкционированного доступа, для создания и хранения которых используется СЭП.

5.1.11. Обеспечить уникальность серийных номеров создаваемых сертификатов ключей проверки электронной подписи.

5.1.12. Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Операторов Удостоверяющего центра и Пользователей Удостоверяющего центра.

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

5.1.14. Обеспечить прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в соответствии с порядком, определенным в Регламенте Уполномоченной организации.

5.1.15. Прекратить действие сертификатов ключей проверки электронной подписи Оператора Удостоверяющего центра и Пользователя Удостоверяющего центра, если истек установленный

срок, на который действие данного сертификата ключа проверки электронной было приостановлено.

5.1.16. Прекратить действие сертификатов ключей проверки электронной подписи Оператора Удостоверяющего центра и Пользователя Удостоверяющего центра в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого были созданы сертификаты ключей проверки электронной подписи Операторов Удостоверяющего центра и Пользователей Удостоверяющего центра.

5.1.17. Официально уведомить о прекращении (аннулировании), приостановлении и возобновлении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации списка отозванных сертификатов ключей проверки электронных подписей.

5.1.18. Публиковать актуальный список отозванных сертификатов ключей проверки электронной подписи на сайте Удостоверяющего центра в ресурсе: http://q.cryptopro.ru/ra/cdp/. Период публикации списка отозванных сертификатов ключей проверки электронных подписей в рабочее время Удостоверяющего центра – 1 (один) час.

5.1.19. Предоставить Уполномоченной организации на согласование и утверждение перечень параметров функционирования СЭП для настройки доступа Операторов и Пользователей УЦ по форме в соответствии с Приложением № 13 к настоящему Регламенту.

5.1.20. Предоставить Уполномоченной организации необходимые права для:

5.1.20.1. осуществления регистрации пользователей в Удостоверяющем центре, формированию и отправке в Удостоверяющий центр заявок в электронной форме на создание и управление сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра;

5.1.20.2. управления доступом Пользователей Удостоверяющего центра к СЭП, в том числе с использованием многофакторной аутентификации;

5.1.20.3. подключения к СЭП Стороннего центра идентификации в соответствии с п. 8.9 настоящего Регламента;

5.1.20.4. подключения SMS-шлюза Уполномоченной организация к СЭП в соответствии с п. 8.10 настоящего Регламента.

5.1.20.5. управления уведомлениями Пользователей Удостоверяющего центра посредством информационных сообщений, в том числе посредством собственного SMS-шлюза;

5.1.20.6. подключения Информационных систем Уполномоченной организации к СЭП с использованием Прикладного интерфейса, предоставляемого Удостоверяющим центром;

5.1.21. Зарегистрировать в СЭП Оператора подключенного Стороннего центра идентификации Уполномоченной организации в соответствии с заявлением по форме Приложения 14 к настоящему Регламенту, полученного от Уполномоченной организации.

5.1.22. Зарегистрировать в СЭП и обеспечить конфиденциальность информации, содержащейся в полученном от Уполномоченной организации файле инициализации OTP-токенов.

5.1.23. В случае отсутствия подключения к СЭП SMS-шлюза Уполномоченной организации осуществлять информирование Пользователей Удостоверяющего центра посредством отправки информационных сообщений на номер мобильного телефона Пользователя Удостоверяющего центра при выполнении операций в СЭП от имени Пользователя Удостоверяющего центра в соответствии с настройками СЭП, установленными Уполномоченной организацией. Номер мобильного телефона Пользователя Удостоверяющего центра должен быть зарегистрирован Оператором Удостоверяющего центра в СЭП или передаваться в СЭП Уполномоченной организацией при аутентификации Пользователя Удостоверяющего центра в СЭП. В период использования тестовых сертификатов ключей проверки электронной подписи выполняется эмуляция отправки информационных сообщений на номер мобильного телефона путем записи их в файл и передачи файла по запросу Уполномоченной организации.

5.1.24. Не позже, чем за 30 (Тридцать) рабочих дней информировать Уполномоченную организацию о проведении обновления программного обеспечения ПАК «КриптоПро DSS» СЭП, предоставить доступ к тестовой версии СЭП с обновленным программным обеспечением

и соответствующую ему руководство разработчика на программное обеспечение «КриптоПро DSS». Информирование осуществляется путем отправки электронного сообщения по электронному адресу, указанному в действующем сертификате ключа проверки электронной подписи Оператора СЭП.

5.2. Уполномоченная организация обязана:

5.2.1. Обеспечить защиту подключения своих Информационных систем к СЭП с использованием СКЗИ, совместимых с СКЗИ, используемых Удостоверяющим центром.

5.2.2. После проведения проверки с использованием тестовых сертификатов ключей проверки электронной подписи согласовать и подписать предоставленный Удостоверяющим центром перечень настроенных параметров функционирования СЭП для доступа Операторов Удостоверяющего центра и Пользователей Удостоверяющего центра по форме, установленной в Приложении № 13 к настоящему Регламенту.

5.2.3. Обеспечить многофакторную аутентификацию Пользователей Удостоверяющего центра при управлении доступом к СЭП, в том числе с использованием Стороннего центра идентификации и SMS-шлюза Уполномоченной организации.

5.2.4. Обеспечить конфиденциальность аутентификационных данных Пользователей Удостоверяющего центра и информации, передаваемой в информационных сообщениях посредством SMS-шлюза Уполномоченной организации.

5.2.5. Передать Администратору Удостоверяющего центра файл инициализации OTP-токенов, которые планируется выдавать Пользователям Удостоверяющего центра для выполнения многофакторной аутентификации при осуществлении доступа к СЭП. Файл инициализации передается с электронной подписью Оператора Удостоверяющего центра

5.2.6. Самостоятельно и за свой счет в обязательном порядке предварительно получать от Пользователей Удостоверяющего центра письменное согласие на получение информационных сообщений на номера мобильных телефонов Пользователей Удостоверяющего центра с одноразовыми паролями и уведомлениями о выполняемых СЭП операциях с использованием принадлежащих Операторам и Пользователям Удостоверяющего центра ключей электронной подписи в соответствии с настоящим Регламентом. Письменное согласие на получение информационных сообщений на номера мобильных телефонов Операторов Удостоверяющего центра оформляется в форме Заявления на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра (Приложение №1 к настоящему Регламенту). Письменное согласие на получение информационных сообщений на номера мобильных телефонов Пользователя Удостоверяющего центра оформляется в форме заявления на создание сертификата ключа проверки ЭП Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», в соответствии с Регламентом Уполномоченной организации.

5.2.7. По письменному запросу предоставить Удостоверяющему центру письменное согласие Пользователя Удостоверяющего центра на получение информационных сообщений на номер мобильного телефона Пользователя Удостоверяющего центра в сроки, установленные в запросе Удостоверяющего центра.

5.2.8. Заверять печатью Уполномоченной организации копии сертификатов ключей проверки электронной подписи, созданным Удостоверяющим центрам по заявкам Оператора Удостоверяющего центра, являющимся полномочным лицом Уполномоченной организации.

5.2.9. Уполномоченная организация при выдаче квалифицированного сертификата обязана направить в единую систему идентификации и аутентификации (ЕСИА) сведения о выданном квалифицированном сертификате. Сведения о выданном квалифицированном сертификате должны направляться в ЕСИА по следующему адресу в сети интернет – https://smevgateway.cryptopro.ru/SmevGateway/.

5.2.10. Оператор Удостоверяющего Центра, являющийся полномочным представителем Уполномоченной организации обязан:

5.2.10.1. При взаимодействии со средствами обеспечения деятельности Удостоверяющего центра использовать только те средства, которые были предоставлены Удостоверяющим центром.

5.2.10.2. Обеспечить конфиденциальность ключей электронных подписей.

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

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

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

5.2.10.6. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

5.2.10.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия квалифицированного сертификата ключа проверки электронной подписи, оформленного по форме Приложения №4 к настоящему Регламенту, в Удостоверяющий центр до момента времени официального уведомления о прекращении действия сертификата ключа проверки электронной подписи, либо об отказе в прекращении действия сертификата ключа проверки электронной подписи.

5.2.10.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия квалифицированного сертификата ключа проверки электронной подписи, оформленного по форме Приложения №5 к настоящему Регламенту, в Удостоверяющий центр до момента времени официального уведомления о приостановлении действия сертификата ключа проверки электронной подписи, либо об отказе в приостановлении действия сертификата ключа проверки электронной подписи.

5.2.10.9. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, действие которого прекращено или приостановлено.

5.2.10.10. Для направления в Удостоверяющий центр заявок на создание и проверку усиленных квалифицированных электронных подписей, создание ключей электронной подписи и ключей проверки электронной подписи использовать СЭП и сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

5.3. Удостоверяющий центр имеет право:

5.3.1. Отказать в создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае ненадлежащего оформления заявления на создание квалифицированного сертификата ключа проверки электронной подписи, оформляемого по форме Приложения №1 к настоящему Регламенту.

5.3.2. Отказать в создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае не предоставления и/или ненадлежащего предоставления документов, установленных п. 4.3 настоящего Регламента.

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

возобновление действия квалифицированного сертификата ключа проверки электронной подписи.

5.3.4. Отказать в прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи.

5.3.5. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с обязательным уведомлением Оператора Удостоверяющего центра и указанием причин приостановления действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

5.3.6. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра с обязательным уведомлением Оператора Удостоверяющего центра и указанием причин приостановления действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

5.3.7. Отказать в создании и управлении сертификатами ключей проверки электронной подписи по заявкам Оператора Удостоверяющего центра до момента получения от Уполномоченной организации подписанного перечня параметров функционирования СЭП для настройки прав доступа Операторов Удостоверяющего центра и Пользователей Удостоверяющего центра по форме, указанной в Приложении № 13 к настоящему Регламенту.

5.3.8. Отказать в подключении Стороннего центра идентификации Уполномоченной организации в случае ненадлежащего оформления заявления на подключение Стороннего центра идентификации, оформляемого в соответствии с Приложением №10 к настоящему Регламенту.

5.3.9. Отказать в подключении SMS-шлюза Уполномоченной организации в случае ненадлежащего оформления заявления на подключение SMS-шлюза, оформляемого в соответствии с Приложением № 11 к настоящему Регламенту.

5.3.10. Отказать в регистрации Оператора Стороннего центра идентификации до получения надлежащим образом оформленного заявления на подключение Стороннего центра идентификации Уполномоченной организации по форме, установленной в Приложении №10 к настоящему Регламенту, или в случае ненадлежащего оформления заявления на регистрацию Оператора СЦИ, оформляемого в соответствии с Приложением № 14 к настоящему Регламенту.

5.3.11. Отказать в предоставлении доступа к СЭП Пользователям Удостоверяющего центра, не прошедшим аутентификацию и не подтвердившим выполнение операций с использованием ключа аутентификации в мобильном приложении myDSS или одноразового пароля.

5.4. Уполномоченная организация имеет право:

5.4.1. Осуществлять с использованием Прикладного интерфейса, предоставляемого Удостоверяющим центром, подключение собственных Информационных систем к СЭП для получения доступа к функциям, необходимым для создания Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи, а также проверки Уполномоченной организацией электронной подписи, управления Уполномоченной организацией ключами электронной подписи и сертификатами ключей проверки электронной подписи.

5.4.2. Осуществлять в соответствии с п.8.7 настоящего Регламента подключение к СЭП собственных Сторонних центров идентификации для управления доступом Операторов Удостоверяющего центра и Пользователей Удостоверяющего центра к СЭП.

5.4.3. Подать в Удостоверяющий центр заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации по форме, установленной Приложением № 14 к настоящему Регламенту.

5.4.4. Осуществить в соответствии с п.8.8 настоящего Регламента подключение к СЭП собственного SMS-шлюза для отправки Пользователям Удостоверяющего центра

информационных сообщений с одноразовыми паролями и уведомлениями о выполняемых СЭП операциях с использованием принадлежащих им ключей электронной подписи.

5.4.5. Предоставлять Пользователям Удостоверяющего центра совместимые со средствами Удостоверяющего центра OTP-токены для многофакторной аутентификации при осуществлении доступа к СЭП.

5.4.6. Предоставлять Пользователям Удостоверяющего центра возможность установки мобильного приложения myDSS из состава ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» версии 2.0» на устройства Пользователей Удостоверяющего центра и создавать им ключ аутентификации для выполнения многофакторной аутентификации при осуществлении доступа к СЭП.

5.4.7. Осуществлять посредством Прикладного интерфейса, предоставляемого Удостоверяющим центром, выгрузку системных журналов аудита операций, совершаемых Пользователями Удостоверяющего центра при получении доступа к СЭП.

5.4.8. Делегировать Пользователям Удостоверяющего центра право подачи заявки в Удостоверяющий центр на создание и управление своими квалифицированными сертификатами ключей проверки электронной подписи посредством Веб- или Прикладного интерфейса СЭП, предоставляемых Удостоверяющим центром. Предоставленные Уполномоченной организацией права Пользователей Удостоверяющего центра определяются параметрами функционирования СЭП в соответствии с Приложением № 13 к настоящему Регламенту и соглашением, заключённым Уполномоченной организацией и Пользователем Удостоверяющего центра. Уполномоченная организация несет всю ответственность за создаваемые Удостоверяющим центром квалифицированные сертификаты ключей проверки электронной подписи по заявкам Пользователей Удостоверяющего центра в соответствии с предоставленными им Уполномоченной организацией правами.

5.4.9. Пользоваться сервисами Службы актуальных статусов сертификатов и Службы штампов времени при использовании СЭП.

5.4.10. Оператор Удостоверяющего центра имеет право:

5.4.10.1. Получить копию сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра на бумажном носителе, заверенную Удостоверяющим центром.

5.4.10.2. Заверять собственноручной подписью копии сертификатов ключей проверки электронной подписи, решение по созданию которых было принято Оператором Удостоверяющего центра.

5.4.10.3. Принимать решения о подаче в Удостоверяющий центр заявки на создание и выдачу сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.4.10.4. Принимать решения о подаче в Удостоверяющий центр заявок на прекращение, приостановление и возобновление действия сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, созданных Удостоверяющим центром по заявкам Оператора Удостоверяющего центра.

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

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

5.4.10.7. Применять список отозванных сертификатов ключей проверки электронных подписей, созданный Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

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

# 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 ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра и Оператора Удостоверяющего центра только в случае, если данные убытки возникли при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра и (или) нарушения конфиденциальности ключа электронной подписи Пользователя Удостоверяющего центра в случае, когда для хранения этого ключа используется СЭП и нарушение конфиденциальности ключа произошла по вине Удостоверяющего центра.

6.5. Вся ответственность за недостоверные данные о Пользователе Удостоверяющего центра, предоставленные Уполномоченной организацией Удостоверяющему центру через СЭП, необходимые для занесения в сертификаты ключей проверки электронной подписи Пользователей Удостоверяющего центра, принятию решений по созданию, выдаче и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, формированию с использованием СЭП копий сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра полностью возлагается на Уполномоченную организацию.

6.6. Вся ответственность по обеспечению конфиденциальности ключа аутентификации при передаче Пользователю Удостоверяющего центра для использования в мобильном приложении myDSS из состава ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» версии 2.0» возлагается на Уполномоченную организацию.

6.7. Вся ответственность по достоверной аутентификации и управлению доступом Пользователей Удостоверяющего центра к Сервису электронной подписи при использовании стороннего центра идентификации и (или) SMS-шлюза полностью возлагается на Уполномоченную организацию, за исключением случаев, когда аутентификация Пользователей Удостоверяющего центра осуществляется с использованием ключа электронной подписи Пользователя Удостоверяющего центра.

6.8. Вся ответственность по подключению Информационных систем Уполномоченной Организации к Сервису электронной подписи полностью возлагается на Уполномоченную организацию.

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

6.10. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется условиями соответствующего Договора и законодательством Российской Федерации.

## 7. Разрешение споров

7.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий Центр и 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. Общий порядок пользования услугами Удостоверяющего центра

Уполномоченная организация в лице Оператора Удостоверяющего центра осуществляет принятие решений по созданию и управлению сертификатами ключей проверки электронной подписи и направляет соответствующие заявки в Удостоверяющий центр с использованием СЭП

Удостоверяющий центр осуществляет действия по формированию ключей электронной подписи, по созданию и управлению сертификатами ключей проверки электронной подписи по заявкам, направленным Оператор Удостоверяющего центра в электронной форме, формируемым в СЭП Оператором Удостоверяющего центра.

Для взаимодействия с Удостоверяющим центром Уполномоченная организация в лице Оператора Удостоверяющего центра должна стать владельцем сертификата ключа проверки электронной подписи.

Формирование ключей электронной подписи, создание, выдача и управление сертификатами Операторов Удостоверяющего центра осуществляется в соответствии с настоящим разделом настоящего Регламента.

8.2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра осуществляется на основании заявления на создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра и доверенности Оператора Удостоверяющего центра. Форма заявления на создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра приведена в Приложении № 1 к настоящему Регламенту, форма доверенности Оператора Удостоверяющего центра приведена в Приложении № 2 к настоящему Регламенту.

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

- Оператором Удостоверяющего центра лично;
- Представителем Уполномоченной организации на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, оформленной по форме Приложения № 3 к настоящему Регламенту;

Администратор Удостоверяющего центра на основе предоставленных заявительных документов выполняет действия по формированию ключа электронной подписи и созданию сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра. Ключ электронной подписи и сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра записываются на предоставляемый заявителем ключевой носитель.

Администратор Удостоверяющего центра передает сформированный ключевой носитель заявителю и распечатывает на бумажном носителе информацию, содержащуюся в созданном сертификате ключа проверки электронной подписи, представленную в виде копии сертификата ключа проверки электронной подписи, оформленной по форме Приложения № 9 к настоящему Регламенту. Заявитель под расписку ознакамливается с информацией из сертификата ключа проверки электронной подписи.

Дополнительно, по согласованию с заявителем, Администратором Удостоверяющего центра сообщается ключевая фраза, использующаяся для аутентификации Оператора Удостоверяющего центра при выполнении регламентных процедур, возникающих при нарушении конфиденциальности ключевых документов Оператора Удостоверяющего центра.

Создание и выдача сертификатов ключей проверки электронной подписи Оператору Удостоверяющего центра осуществляется Удостоверяющим центром в день прибытия

заявителя. День прибытия заявителя согласовывается с Администратором Удостоверяющего центра. Удостоверяющий центр вправе отказать в создании сертификатов ключей проверки электронной подписи Оператору Удостоверяющего центра по заявлениям, поступившим в Удостоверяющим центр без согласования дня прибытия заявителя.

8.3. Прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Удостоверяющий центр прекращает действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в следующих случаях:

- при прекращении действия настоящего Регламента в отношении Уполномоченной организации по усмотрению Удостоверяющего центра;
- по истечении срока, на который действие сертификата ключа проверки электронной подписи было приостановлено;
- по заявлению владельца сертификата ключа проверки электронной подписи;
- в связи с аннулированием сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу;
- по истечении срока действия сертификата ключа проверки электронной подписи;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи.

В случае прекращения действия настоящего Регламента, истечения срока, на который действие сертификата ключа проверки электронной подписи было приостановлено, по заявлению владельца сертификата ключа проверки электронной подписи, по решению суда, вступившего в законную силу, Удостоверяющий центр официально уведомляет владельца сертификата ключа проверки электронной подписи и всех Пользователей Удостоверяющего центра о прекращении действия сертификата ключа проверки электронной подписи не позднее одного рабочего дня с момента наступления описанного события.

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

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

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

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

8.3.1. Прекращение действия сертификата ключа проверки электронной подписи по заявлению Оператора Удостоверяющего центра

Подача заявления на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по форме Приложения № 4 к настоящему Регламенту может быть осуществлена посредством отправления заявление на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра почтовой или курьерской связью.

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

В случае отказа в прекращении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Удостоверяющий центр уведомляет об этом Оператора Удостоверяющего центра с указанием причин отказа.

При принятии положительного решения о прекращении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Администратор Удостоверяющего центра осуществляет прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

8.4. Приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

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

- по заявлению владельца сертификата ключа проверки электронной подписи;
- по заявке владельца сертификата ключа проверки электронной подписи в устной форме в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

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

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра действие этого сертификата ключа проверки электронной подписи не будет возобновлено, то данный сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра прекращает своё действие.

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

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

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

8.4.1. Приостановление действия сертификата ключа проверки электронной подписи по заявлению Оператора Удостоверяющего центра

Подача в Удостоверяющий центр заявления на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по форме Приложения № 5 настоящего Регламента может быть осуществлена посредством отправления заявление на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра почтовой или курьерской связью.

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

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

При принятии положительного решения о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Администратор Удостоверяющего центра осуществляет приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра на срок, указанный в заявлении на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

8.4.2. Приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по заявке в устной форме

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

Заявка подается в Удостоверяющий центр по телефону.

Оператор Удостоверяющего центра должен сообщить Администратору Удостоверяющего центра следующую информацию:

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

Заявка о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра принимается Удостоверяющим центром только в случае положительной аутентификации Оператора Удостоверяющего центра (совпадения ключевой фразы, сообщенной Оператором Удостоверяющего центра по телефону, и ключевой фразы, определенной при создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, хранящейся в Удостоверяющем центре).

После принятия заявки о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Администратор Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, которое должно быть осуществлено

в течение рабочего дня поступления заявки о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

В случае отказа в приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Удостоверяющий центр уведомляет об этом Оператора Удостоверяющего центра с указанием причины отклонения заявки.

При принятии положительного решения о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Администратор Удостоверяющего центра приостанавливает действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра до окончания срока действия ключа электронной подписи, соответствующего данному сертификату ключа проверки электронной подписи Оператора Удостоверяющего центра.

Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Оператор Удостоверяющего центра должен предоставить в Удостоверяющий центр заявление на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра (в том случае, если факт нарушения конфиденциальности ключа электронной подтвердился), либо заявление на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра (в том случае, если нарушения конфиденциальности ключа электронной подписи не было).

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

Удостоверяющий центр вправе приостановить действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случаях нарушения конфиденциальности или подозрения в нарушении конфиденциальности соответствующего ключа электронной подписи в том случае, если Оператору Удостоверяющего центра не было известно о возможном факте нарушения конфиденциальности ключей, а также в случаях неисполнения Оператором Удостоверяющего центра обязательств по настоящему Регламенту, до окончания срока действия ключа электронной подписи, соответствующего данному сертификату ключа проверки электронной подписи Оператора Удостоверяющего центра.

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

8.5. Возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра только по заявлению на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, оформленного по форме Приложения № 6 к настоящему Регламенту, подписанному владельцем сертификата ключа проверки электронной подписи и только в том случае, если действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра было приостановлено.

Подача в Удостоверяющий центр заявления на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра может быть осуществлена посредством направления заявления на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра почтовой или курьерской связью.

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

сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра было принято Удостоверяющим центром.

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

При принятии положительного решения о возобновлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Администратор Удостоверяющего центра осуществляет возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

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

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

8.6. Подключение Информационной системы Уполномоченной Организации к Сервису электронной подписи

Удостоверяющий центр предоставляет Уполномоченной организации Прикладной интерфейс подключения к Сервису электронной подписи в соответствии с руководством разработчика на программное обеспечение «КриптоПро DSS». Защита передаваемых от Информационной системы к Сервису электронной подписи данных осуществляется в соответствии с требованиями Уполномоченной Организации с использованием СКЗИ, совместимых со средствами Удостоверяющего центра.

8.7. Подключение Стороннего центра идентификации Уполномоченной организации к Сервису электронной подписи

Подключение Стороннего центра идентификации Уполномоченной организации к Сервису электронной подписи осуществляется в соответствии с документацией на программное обеспечение «КриптоПро DSS» по заявлению на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО», оформляемому по форме Приложения №10 к настоящему Регламенту, от Уполномоченной Организации. Заявление на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО» направляется в Удостоверяющий центр курьерской или почтовой связью. Вместе с заявлением на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО» на носителе информации передается сертификат, используемый для проверки подписи SAML-токенов, передаваемых от Стороннего центра идентификации.

Сторонний центр идентификации Уполномоченной организации подключается к Сервису электронной подписи на период действия предоставленного сертификата Стороннего центра идентификация при условии предоставления Удостоверяющему центру необходимых заявлений, указанных в настоящем пункте Регламента.

При смене Уполномоченной организацией сертификата Стороннего центра идентификации осуществляется повторное подключение Стороннего центра идентификации Уполномоченной организации к Сервису электронной подписи в соответствии с настоящим пунктом Регламента.

Заявление на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО» и сертификат Стороннего центра идентификации могут быть отправлены Администратору Удостоверяющего центра в электронной форме, подписанные электронной подписью Оператора УЦ и руководителя Уполномоченной организации с использованием сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

Регистрацию Оператора СЦИ в СЭП выполняет Удостоверяющий центр после получения заявления на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации, оформленного по форме Приложения №14 к настоящему Регламенту и доверенности Оператора Стороннего центра идентификации Уполномоченной организации. Форма доверенности Оператора Стороннего центра идентификации Уполномоченной организации устанавливается в Приложении №15 к настоящему Регламенту. Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации и доверенность Оператора Стороннего центра идентификации Уполномоченной организации направляются в Удостоверяющий центр курьерской или почтовой связью.

Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации может быть отправлено Администратору Удостоверяющего центра в электронной форме, подписанное электронной подписью Оператора УЦ и руководителя Уполномоченной организации с использованием сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

8.8. Подключение SMS-шлюза Уполномоченной Организации к Сервису электронной подписи

Подключение SMS-шлюза Уполномоченной Организации к Сервису электронной подписи осуществляется в соответствии с документацией на программное обеспечение «КриптоПро DSS» по заявлению на подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи ООО «КРИПТО-ПРО», оформляемому по форме Приложения №11 к настоящему Регламенту, полученному от Уполномоченной Организации. Заявление на подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи ООО «КРИПТО-ПРО» направляется в Удостоверяющий центр курьерской или почтовой связью.

Заявление на подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи ООО «КРИПТО-ПРО» может быть отправлено Администратору Удостоверяющего центра в электронной форме, подписанное электронной подписью Оператора УЦ и руководителя Уполномоченной организации с использованием сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

Защита передаваемых от Сервиса электронной подписи на SMS-шлюз Уполномоченной Организации информационных сообщений осуществляется в соответствии с требованиями Уполномоченной Организации с использованием СКЗИ, совместимых со средствами Удостоверяющего центра.

8.9. Получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром

Проверка актуального статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром по заявкам, направленным Уполномоченной организацией, осуществляется с использованием СЭП.

Получение документированной информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется на основании заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО», оформляемого по форме Приложения № 7 к настоящему Регламенту, направляемого Оператором Удостоверяющего центра в Удостоверяющий центр. Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО» направляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО», должно содержать следующую информацию:

- время и дата подачи заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО»;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа проверки электронной подписи;
- идентификационные данные Пользователя Удостоверяющего центра, статус сертификата ключа проверки электронной подписи которого требуется установить;
- серийный номер сертификата ключа проверки электронной подписи, статус которого требуется установить.

По результату проведения проверки актуального статуса сертификата ключей проверки электронной подписи по заявлению на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО», оформляется Удостоверяющим центром справка, содержащая информацию о статусе сертификата ключа проверки электронной подписи, которая предоставляется Оператору Удостоверяющего центра.

Предоставление Оператору Удостоверяющего центра справки, содержащую информацию о статусе сертификата ключа проверки электронной подписи, должно быть осуществлено не позднее 10 (десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО».

## 8.10. Подтверждение подлинности электронной подписи в электронном документе

Проверка электронной подписи, созданной средствами СЭП, осуществляется с использованием СЭП и (или) локальными средствами электронной подписи, совместимыми со средствами СЭП.

По запросу Уполномоченной Организации, Удостоверяющий центр осуществляет оказание услуг по подтверждению подлинности электронной подписи в электронном документе, созданной с использованием Сервиса электронной подписи.

В том случае, если формат электронного документа с ЭП соответствует стандарту криптографических сообщений, реализуемых Сервисом электронной подписи, то Удостоверяющий центр обеспечивает подтверждение подлинности ЭП в электронном документе. Решение о соответствии электронного документа с ЭП поддерживаемым СЭП стандартам принимает Удостоверяющий центр.

Для подтверждения подлинности ЭП в электронных документах Оператор удостоверяющего центра подает заявление на подтверждение подлинности электронной подписи в электронном документе, оформляемого по форме Приложения № 8 к настоящему Регламенту, в Удостоверяющий центр.

Заявление на подтверждение подлинности электронной подписи в электронном документе должно содержать следующую информацию:

- дата и время подачи заявления на подтверждение подлинности электронной подписи в электронном документе;
- идентификационные данные Пользователя Удостоверяющего центра, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является CD(DVD) или flash-носитель, содержащий:

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

Оказание услуг по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом оказания услуг по подтверждению подлинности ЭП в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

- состав комиссии, осуществлявшей проверку ЭП в электронном документе;
- основание для проведения проверки ЭП в электронном документе;
- результат проверки ЭП в электронном документе;
- данные, представленные комиссии для проведения проверки ЭП в электронном документе;
- отчет по выполненной проверке ЭП в электронном документе.

Отчет по выполненной проверке ЭП в электронном документе содержит:

- время и место проведения проверки ЭП в электронном документе;
- содержание и результаты проверки ЭП в электронном документе;
- обоснование результатов проверки ЭП в электронном документе.

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

Срок оказания услуг по подтверждению подлинности ЭП в одном электронном документе и предоставлению Уполномоченной организации заключения Удостоверяющего центра по выполненной проверке ЭП в электронном документе составляет 10 (десять) рабочих дней с момента поступления заявления на подтверждение подлинности электронной подписи в электронном документе в Удостоверяющий центр.

В том случае, если ЭП сформирована без использования Сервиса электронной подписи, то оказание услуг по подтверждению подлинности ЭП в электронном документе осуществляется в рамках заключения отдельного договора (соглашения) между Удостоверяющим центром и Уполномоченной Организацией. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки оказания услуг, размер вознаграждения Удостоверяющего центра, а также иные условия, определяются договором (соглашением) между Удостоверяющим центром и Уполномоченной Организацией.

8.11. Регистрация Пользователей Удостоверяющего центра, управление сертификатами ключей проверки электронной подписи Пользователей УЦ, управление доступом к СЭП

Регистрация Пользователей Удостоверяющего центра, принятие решений по созданию сертификатов ключей проверки электронной подписи Пользователей УЦ и управлению сертификатами ключей проверки электронной подписи Пользователей УЦ, формирование копий сертификатов ключей проверки электронной подписи Пользователей УЦ производится Оператором Удостоверяющего центра и осуществляется в соответствии с порядком, установленным Уполномоченной организацией.

Удостоверяющий центр выполняет действия по созданию сертификатов ключей проверки электронной подписи Пользователя УЦ, прекращению действия сертификатов ключей проверки электронной подписи Пользователя УЦ, приостановлению и возобновлению действий сертификатов ключей проверки электронной подписи Пользователя УЦ в соответствии с настройками параметров функционирования СЭП, определенных в Перечне параметров функционирования Сервиса электронной подписи ООО «КРИПТО-ПРО» для настройки доступа Операторов УЦ и Пользователей УЦ, оформляемом по форме Приложения №13, на основании заявок в электронной форме внутреннего формата СЭП, направляемых

Оператором Удостоверяющего центра и (или) Пользователями Удостоверяющего центра с использованием Веб- или Прикладного интерфейса СЭП, предоставляемого Удостоверяющим центром. Выполнение указанных действий осуществляется Удостоверяющим центром при соответствии параметров аутентификации заявителя регистрационным данным:

- Подтвержден уникальный идентификатор Центра идентификации СЭП или Стороннего центра идентификации Уполномоченной организации, в котором зарегистрирован Оператор Удостоверяющего центра и (или) Пользователь Удостоверяющего центра;
- Сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра на момент получения заявки Удостоверяющим центром действителен и содержит в расширении ExtendedKeyUsage область использования – Оператор DSS (1.2.643.2.2.34.32) или идентификатор Оператора УЦ получен от Стороннего центра идентификации Уполномоченной организации.
- Аутентификация Пользователя УЦ подтверждена с использованием ключа аутентификации в мобильном приложении (программе для ЭВМ) «КриптоПро myDSS» или СКЗИ «КриптоПро CSP» на рабочем месте Пользователя УЦ или одноразовым паролем, переданного заявителю от СЭП посредством информационного сообщения или сформированным им с использованием OTP-токена, полученного от Оператора Удостоверяющего центра.

Регистрация всех операций, выполняемых Операторами Удостоверяющего центра и Пользователями Удостоверяющего центра, осуществляется средствами СЭП. Журналы аудита для контроля и анализа выполненных операций, разрешения спорных вопросов и конфликтных ситуаций, связанных с использованием СЭП, предоставляются Удостоверяющим центром по запросу Уполномоченной организации.

Доступ Пользователей Удостоверяющего центра к Сервису электронной подписи осуществляется посредством Веб- или Прикладного интерфейса, предоставляемого Удостоверяющим центром, на основании аутентификационной информации, переданной Уполномоченной организацией при регистрации и подключении Пользователя УЦ в СЭП или полученной от Стороннего центра идентификации Уполномоченной организации.

Функции создания электронной подписи посредством Сервиса электронной подписи доступны владельцам действующих сертификатов ключей проверки электронной подписи Пользователя УЦ, созданных Удостоверяющим центром по заявкам, направленным Уполномоченной организацией.

Владелец сертификата ключа проверки электронной подписи Пользователя УЦ подтверждает использование своего ключа электронной подписи посредством мобильного приложения (программы для ЭВМ) «КриптоПро myDSS» или СКЗИ «КриптоПро CSP» на рабочем месте Пользователя УЦ или одноразового пароля, формируемого СЭП и отправляемого в информационном сообщении на номер мобильного телефона владельца сертификата ключа проверки электронной подписи Пользователя УЦ, указанный при регистрации Пользователя Удостоверяющего центра. Одноразовый пароль для подтверждения операций с ключом электронной подписи может быть сформирован OTP-токеном, выдаваемым владельцу соответствующего сертификата ключа проверки электронной подписи Оператором УЦ по заявлению Пользователя Удостоверяющего центра.

8.12. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени при использовании СЭП

Удостоверяющий центр предоставляет актуальную информации о статусе сертификатов ключа проверки электронной подписи при использовании СЭП посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра посредством СЭП формирует и предоставляет этим Пользователям Удостоверяющего центра OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи Службы актуальных

статусов сертификатов (Оператора Службы актуальных статусов сертификатов). OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭП 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 ЭП OCSP-ответа действителен;
- Ключ электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении ExtendedKeyUsage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);
- Сертификат ключа проверки электронной подписи, статус которого установлен с использованием данного OCSP-ответа, издан Удостоверяющим центром и содержит в расширении ExtendedKeyUsage или ApplicationPolicy 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 AuthorityInformationAccess (AIA) издаваемых Удостоверяющим центров сертификатов ключей проверки электронной подписей.

Удостоверяющий центр предоставляет штампы времени при использовании СЭП посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному ЭП электронному документу, признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭП Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- Сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭП штампа времени действителен;
- Ключ электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;
- Сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) содержит в расширении ExtendedKeyUsage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);
- Сертификат ключа проверки электронной подписи, на котором сформирована ЭП электронного документа и к которому относится данный штамп времени, издан Удостоверяющим центром и содержит в расширении ExtendedKeyUsage или ApplicationPolicy 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.

8.13. Порядок оказания технической поддержки СЭП.

8.13.1. Удостоверяющий центр оказывает техническую поддержку СЭП на основании сертификата технической поддержки СЭП.

8.13.2. Сертификат технической поддержки СЭП выдается Уполномоченной организации при подключении. Сертификат технической поддержки СЭП должен быть зарегистрирован на портале технической поддержки Удостоверяющего центра по адресу: https://support.cryptopro.ru.

8.13.3. Удостоверяющий центр оказывает круглосуточную техническую поддержку СЭП через портал технической поддержки https://support.cryptopro.ru.

8.13.4. Представитель Уполномоченной организации направляет в Удостоверяющий центр обращение через портал технической поддержки https://support.cryptopro.ru с указанием своей идентифицирующей информации (фамилия, имя и отчество физического лица, представляющее интересы и выступающего от имени Уполномоченной организации; наименование Уполномоченной организации), регистрационного номера сертификата технической поддержки СЭП и описанием инцидента или вопроса.

8.13.5. Обращение должно содержать следующую информацию:

- Тема сообщения с префиксом «SaaS. <Наименование Уполномоченной организации>»
- Дата и время (или диапазон времени) возникновения ошибки
- Интерфейс взаимодействия с СЭП (API или веб)
- Процесс, на котором возникает ошибка (регистрация пользователя, назначение аутентификации, получение/обновление/отзыв сертификата, подписание документа и т.п.)
- Логин пользователя в СЭП (опционально)
- Логин оператора в СЭП (опционально)
- Описание инцидента
- Возвращаемая ошибка со стороны СЭП
- Дополнительная информация при необходимости.

8.13.6. Сотрудник службы технической поддержки СЭП регистрирует обращение через Портал технической поддержки, направляя лицу, создавшему обращение, электронное сообщение по электронной почте с номером зарегистрированного обращения для идентификации обращения.

8.13.7. Время реакции Удостоверяющего центра на обращение определяется степенью критичности инцидента, присвоенной при регистрации обращения или в процессе работы над инцидентом. Первоначально присвоенная степень критичности может быть изменена в процессе работы над инцидентом при согласовании такого изменения в рабочем порядке.

8.13.8. Время реакции на критические инциденты составляет 2 часа.

8.13.9. Время реакции на некритичные инциденты составляет 8 часов.

8.13.10. При отсутствии реакции Уполномоченной организации на предложенное службой технической поддержки Удостоверяющего центра решение или запрос дополнительной информации в течение 3 (трех) рабочих дней с даты получения представителем Уполномоченной организации соответствующего решения или запроса от Службы технической поддержки Удостоверяющего центра, обращение считается неактуальным. Услуги Удостоверяющего центра по технической поддержке СЭП по обращению считаются своевременно оказанными, а само обращение - закрытым. При поступлении информации от Уполномоченной организации по закрытому обращению, такое обращение снова открывается или регистрируется как новое обращение.

8.13.11. Если в процессе работы над инцидентом сотрудник службы технической поддержки СЭП выясняет, что инцидент связан с продуктом стороннего производителя и (или) вызван сторонней информационной системой, то Уполномоченной организации рекомендуется обратиться в службу технической поддержки соответствующего производителя.

# 9. Форма сертификата ключей проверки электронной подписи и сроки действия ключевых документов

9.1. Форма сертификата ключа проверки электронной подписи, создаваемого и выдаваемого Удостоверяющим центром

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

Дополнительно в создаваемые и выдаваемые сертификаты ключей проверки электронной подписи может быть занесено:

- в поле Subject (идентифицирует владельца сертификата ключа проверки электронной подписи):
  - Поле E (Email) – адрес электронной почты;
  - Поле T (Title) – должность полномочного представителя юридического лица, данные которого занесены в сертификат ключа проверки электронной подписи наряду с наименованием юридического лица (если владелец сертификата ключа проверки электронной подписи – юридическое лицо);
- расширение Private Key Validity Period – срок действия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи, следующего формата:

  Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;

  Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;
- расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) – набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с сертификатом ключа проверки электронной подписи (если такие ограничения установлены);
- расширение CRL Distribution Point (Точка распространения списка отозванных сертификатов ключей проверки электронной подписи) - набор адресов точек распространения списков отозванных сертификатов ключей проверки электронной подписи;
- расширение Authority Information Access (Доступ к информации о центре) – Адрес обращения к Службе актуальных статусов сертификатов, Адрес размещения сертификата ключа проверки электронной подписи Удостоверяющего центра;
- иные поля и расширения по усмотрению Удостоверяющего центра.

9.2. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

| Название | Описание | Содержание |
|---|---|---|
| **Базовые поля списка отозванных сертификатов** | | |
| Version | Версия | V2 |
| Issuer | Издатель СОС | Идентификационные данные Удостоверяющего центра |
| 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<br>1. Серийный номер сертификата (CertificateSerialNumber)<br>2. Время обработки заявления на аннулирование (отзыв) сертификата (Time)<br>3. Код причины отзыва сертификата (ReasonCode)<br>"0" Не указана<br>"1" Компрометация ключа<br>"2" Компрометация ЦС<br>"3" Изменение принадлежности<br>"4" Сертификат заменен<br>"5" Прекращение работы<br>"6" Приостановка действия |

| | | |
|---|---|---|
| signatureAlgorithm | Алгоритм подписи | ГОСТ Р 34.11/34.10-2012 |
| signatureValue | Подпись издателя СОС | Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012 |
| **Расширения списка отозванных сертификатов (crlExtensions)** | | |
| Authority Key Identifier | Идентификатор ключа издателя | Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС |
| CRL Number | Номер CRL | Порядковый номер СОС |
| SzOID_CertSrv_CA_Version | Объектный идентификатор сертификата издателя | Версия сертификата ключа проверки электронной подписи Удостоверяющего Центра |

9.3. Сроки действия ключевых документов

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

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

Срок действия сертификата ключа проверки электронной подписи (корневого сертификата ключа проверки электронной подписи) Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи (корневого сертификата ключа проверки электронной подписи) Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «ValidityPeriod» соответственно.

Срок действия ключа электронной подписи Службы актуальных статусов сертификатов составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

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

Срок действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

Срок действия ключа электронной подписи Службы штампов времени составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

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

Срок действия сертификата ключа проверки электронной подписи Службы штампов времени не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы штампов времени и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

В том случае, если федеральным законом либо иным нормативно-правовым актом Российской Федерации устанавливается досрочное прекращение действия сертификатов ключей проверки электронной подписи, то действие данных сертификатов ключей проверки электронной подписи прекращается в силу и в соответствии с положениями федерального закона либо иного нормативно-правового акта Российской Федерации.

9.3.2. Сроки действия ключевых документов Оператора Удостоверяющего центра и Пользователя Удостоверяющего центра

Срок действия ключа электронной подписи Оператора Удостоверяющего центра и Пользователя Удостоверяющего центра составляет 1 (Один) год.

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

Срок действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра и Пользователя Удостоверяющего центра не превышает 12 (пятнадцать) месяцев. Время начала периода действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра и Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

В том случае, если федеральным законом либо иным нормативно-правовым актом Российской Федерации устанавливается досрочное прекращение действия сертификатов ключей проверки электронной подписи, то действие данных сертификатов ключей проверки электронной подписи прекращается в силу и в соответствии с положениями федерального закона либо иного нормативно-правового акта Российской Федерации.

# 10. Дополнительные положения

10.1. Плановая смена ключей электронной подписи Удостоверяющего Центра

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

Процедура плановой смены ключей электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр создает новый сертификат ключа проверки электронной подписи.

Уведомление Операторов Удостоверяющего центра и Пользователей Удостоверяющего центра о проведении смены ключей Удостоверяющего центра осуществляется посредством электронной почты.

Старый ключ электронной подписи Удостоверяющего центра используется для формирования списков отозванных сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром в период действия старого ключа электронной подписи Удостоверяющего центра.

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

10.2. Компрометация (нарушение конфиденциальности) ключевых документов Удостоверяющего центра, внеплановая смена ключей электронной подписи Удостоверяющего центра

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра действие сертификат ключа проверки электронной подписи Удостоверяющего Центра прекращается, Операторы Удостоверяющего центра и Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации (нарушении конфиденциальности) ключа электронной подписи Удостоверяющего центра на сайте Удостоверяющего центра. Все сертификаты ключей проверки электронной подписи, подписанные с использованием скомпрометированного ключа Удостоверяющего центра, считаются прекратившими действие.

После прекращения действия сертификата ключа проверки электронной подписи Удостоверяющего Центра выполняется процедура внеплановой смены ключей электронной подписи Удостоверяющего центра. Процедура внеплановой смены ключей электронной подписи Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей электронной подписи Удостоверяющего центра (пункт 10.1 настоящего Регламента).

Все действовавшие на момент компрометации (нарушения конфиденциальности) ключа электронной подписи Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты ключей проверки электронной подписи, действие которых было приостановлено, подлежат внеплановой смене. В случае внеплановой смены ключей

электронной подписи в связи с компрометацией (нарушением конфиденциальности) ключа электронной подписи Удостоверяющего центра оплата за создание сертификатов ключа проверки электронной подписи Оператора Удостоверяющего центра и Пользователей Удостоверяющего центра Удостоверяющим центром не взимается.

10.3. Нарушение конфиденциальности ключевых документов Оператора Удостоверяющего центра

Оператор Удостоверяющего центра самостоятельно принимает решение о факте или угрозе нарушения конфиденциальности своего ключа электронной подписи.

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Оператора Удостоверяющего центра Оператор Удостоверяющего центра связывается с Удостоверяющим центром по телефону и приостанавливает действие сертификата ключа проверки электронной подписи, соответствующего ключу электронной подписи, конфиденциальность которого нарушена, посредством подачи заявки о приостановлении действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра н в устной форме (пункт 8.4.2 настоящего Регламента).

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Оператора Удостоверяющего Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра Оператору УЦ в соответствии с пунктом 8.2 настоящего Регламента.

10.4. Конфиденциальность информации

10.4.1. Типы конфиденциальной информации

10.4.1.1. Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре в качестве владельца сертификата ключа проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключей электронной подписи Операторов Удостоверяющего центра. Пользователи Удостоверяющего центра хранят свои ключи электронной подписи с использованием СЭП.

10.4.1.2. Персональная и корпоративная информация об Операторах Удостоверяющего центра и Пользователях Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной, в том числе информация об операциях осуществляемых с использованием СЭП УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ, и/или УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ, и/или Пользователем Удостоверяющего центра.

10.4.1.3. Информация, передаваемая в составе электронного документа, и (или) информационных сообщений при взаимодействии с СЭП, считается конфиденциальной. Конфиденциальность информационных сообщений обеспечивается средствами оператора мобильной связи и Уполномоченной организации при подключении SMS-шлюза.

10.4.1.4. Информация, содержащаяся в файле инициализации OTP-токенов, передаваемом Уполномоченной организацией Администратору УЦ считается конфиденциальной.

10.4.1.5. Ключи аутентификации в мобильном приложении myDSS из состава ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» версии 2.0», передаваемые Пользователям Удостоверяющего центра, считаются конфиденциальной информацией.

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 проверки электронной подписи и списки отозванных сертификатов ключей проверки электронной подписи, создаваемые Удостоверяющим центром, не считается конфиденциальной.

10.4.2.4. Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, создаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

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 проверки электронной подписи в Удостоверяющем центре

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

10.6. Прекращение оказания услуг Удостоверяющим центром

10.6.1. В случае прекращения действия настоящего Регламента в отношении Уполномоченной организации действие сертификатов ключей проверки электронной подписи Оператора Удостоверяющего центра, как представителя Уполномоченной организации, а также действие сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, решение по созданию и выдаче которых приняла Уполномоченная организация в лице Оператора Удостоверяющего центра, по усмотрению Удостоверяющего центра может быть прекращено. В этом случае от Сервиса электронной подписи отключаются все Сторонние центры идентификации и SMS-шлюз Уполномоченной Организации.

10.7. Непреодолимая сила (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.

10.8. Деятельность Удостоверяющего центра в переходный период, связанный со вступлением в силу поправок в Федеральный закон «Об электронной подписи»

10.8.1. В связи с внесением изменений в Федеральный закон «Об электронной подписи» Федеральным законом от 27.12.2019 г. №476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее – ФЗ № 476-ФЗ) УДОСТОВЕРЯЮЩИЙ ЦЕНТР:

- не гарантирует, что будет аккредитован на соответствие требованиям к аккредитации удостоверяющих центров, установленным Федеральным законом «Об электронной подписи»;
- не гарантирует создание квалифицированных сертификатов ключей проверки электронной подписи в соответствии с требованиями Федерального закона «Об электронной подписи» с 01.07.2021;
- не гарантирует, что средство электронной подписи, с использованием которого обеспечивается эксплуатация Сервиса электронной подписи, будет иметь подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» с 01.07.2021;
- гарантирует управление, созданными ранее квалифицированными сертификатами ключей проверки электронной подписи, а также публикацию списка отозванных квалифицированных сертификатов ключей проверки электронной подписи, хранение информации и информирование владельцев сертификатов ключей проверки электронной подписи согласно п. 2 ст. 15 »Федерального закона «Об электронной подписи» до 01.01.2022.
- уведомляет, что ранее созданные квалифицированные сертификаты ключей проверки электронной подписи прекратят своё действие в случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами (в том числе согласно п. 4 статьи 3 ФЗ №476-ФЗ), а также в соответствии с иными нормативно-правовыми актами Российской Федерации.

10.8.2. Суммы, полученные УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ за оказание услуг по созданию квалифицированных сертификатов ключей проверки электронной подписи, действие которых будет досрочно прекращено в силу федерального закона (в том числе согласно ФЗ №476-ФЗ) либо иного нормативно-правового акта Российской Федерации, не подлежат возврату полностью или частично в связи с своевременным и надлежащим оказанием услуг УДОСТОВРЕЮЩИМ ЦЕНТРОМ.

10.8.3. УДОСТОВЕРЯЮЩИЙ ЦЕНТР не несет ответственность перед УПОЛНОМОЧЕННОЙ ОРГАНИЗАЦИЕЙ и владельцами квалифицированных сертификатов ключей проверки электронной подписи, в том числе не возмещает какие-либо убытки, связанные с прекращением действия квалифицированных сертификатов ключей проверки электронной подписи, действие которых будет досрочно прекращено в силу федерального закона (в том числе согласно ФЗ №476-ФЗ) либо иного нормативно-правового акта Российской Федерации.

# 11. Список приложений

11.1. Приложение № 1. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

11.2. Приложение № 2. Форма доверенности Оператора Удостоверяющего центра.

11.3. Приложение № 3. Форма доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи за Оператора Удостоверяющего центра.

11.4. Приложение № 4. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

11.5. Приложение № 5. Форма заявления на приостановление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

11.6. Приложение № 6. Форма заявления на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра.

11.7. Приложение № 7. Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром.

11.8. Приложение № 8. Форма заявления на подтверждение подлинности электронной подписи в электронном документе.

11.9. Приложение № 9. Форма копии сертификата ключа проверки электронной подписи на бумажном носителе.

11.10. Приложение № 10. Форма заявления на подключение к Сервису электронной подписи Стороннего центра идентификации Уполномоченной Организации.

11.11. Приложение № 11. Форма заявления на подключение к Сервису электронной подписи SMS-шлюза Уполномоченной Организации.

11.12. Приложение № 12. Функции Сервиса электронной подписи.

11.13. Приложение № 13. Перечень параметров функционирования Сервиса электронной подписи для настройки доступа Операторов и Пользователей УЦ.

11.14. Приложение № 14. Форма заявления на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации.

11.15. Приложение № 15. Форма доверенности Оператора Стороннего центра идентификации Уполномоченной организации.

Приложение № 1
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на создание квалифицированного сертификата
ключа проверки электронной подписи Оператора Удостоверяющего центра)

Заявление на создание квалифицированного сертификата
ключа проверки электронной подписи
Оператора Удостоверяющего центра

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

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

действующего на основании _____

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

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

_____
(фамилия, имя, отчество полномочного представителя)

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

| | |
|---|---|
| CommonName (CN) | Наименование организации |
| INN | ИНН организации |
| OGRN | ОГРН организации |
| Organization (O) | Наименование организации |
| Locality (L)<br>StreetAdrdess (STREET)<br>State (S)<br>Contry (C) | Город<br>Улица, номер дома, корпуса, строения, помещения<br>Субъект Российской Федерации<br>Страна=RU<br>Адрес места нахождения организации (согласно юридического или фактического адреса - по усмотрению заявителя) |
| SurName (SN) | Фамилия полномочного представителя – Оператора Удостоверяющего центра, действующего от имени организации |
| GivenName (GN) | Имя и Отчество полномочного представителя |
| Title (T) | Должность полномочного представителя (необязательное поле) |
| OrganizationUnit (OU) | Наименование подразделения полномочного представителя (необязательное поле) |
| E-Mail (E) | Адрес электронной почты полномочного представителя |

Просит использовать адрес электронной почты _____ и (или) номер мобильного телефона для отправки почтовых сообщений и SMS-сообщений через оператора сотовой связи с уведомлением о событиях Сервиса электронной подписи

_____
*Код страны, код региона, номер телефона в формате +X-XXX-XXX-XX-XX*

*(указывается при необходимости такой рассылки)*

Настоящим _____
(фамилия, имя, отчество Оператора Удостоверяющего центра, серия и номер паспорта, кем и когда выдан)
_____ _____

соглашается с обработкой своих персональных данных ООО «КРИПТО-ПРО» и признает, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, относятся к общедоступным персональным данным, а именно: фамилия, имя, отчество; СНИЛС; ИНН; адрес места регистрации (страна, субъект Российской Федерации, населенный пункт, улица, номер дома, корпуса, строения, квартиры); адрес электронной почты; номер телефона. ООО «КРИПТО-ПРО» имеет право обрабатывать мои персональные данные следующими способами: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных. Настоящее согласие на обработку своих персональных данных ООО «КРИПТО-ПРО» дано на срок действия сертификата ключа проверки электронной подписи, а также на 5 (пять) лет после прекращения срока действия сертификата ключа проверки электронной подписи. Настоящим также согласен с получением на вышеуказанный номер мобильного телефона и адрес электронной почты информационных сообщений, одноразовых паролей и уведомлений о выполняемых операциях с использованием выпущенного ключа электронной подписи.

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

_____ _____ /_____/
(Должность руководителя Уполномоченной организации) (подпись) (фамилия, инициалы)

«___»_____20__ г.

М.П.

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

Приложение № 2
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма доверенности Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество представителя)

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

действовать от имени _____
(полное наименование организации)

при использовании электронной подписи электронных документов, выступать в роли Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» и осуществлять действия в рамках Регламента Удостоверяющего центра ООО «КРИПТО-ПРО» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи (Схема обслуживания: распределенная с оператором), установленные для Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

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

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

подтверждаю.

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

Приложение № 3
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма доверенности на получение ключей электронной подписи и сертификата ключа
проверки электронной подписи за Оператора Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество представителя)

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

получить ключ электронной подписи и сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра, созданные для Оператора Удостоверяющего центра

_____
(фамилия, имя, отчество Оператора Удостоверяющего центра)

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

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

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

подтверждаю.

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

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

Приложение № 4
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на прекращение действия сертификата
ключа проверки электронной подписи)

Заявление на прекращение действия сертификата
ключа проверки электронной подписи
Оператора Удостоверяющего центра

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит прекратить действие своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

| | |
|---|---|
| SerialNumber (SN) | Серийный номер сертификата ключа проверки электронной подписи |
| CommonName (CN) | Наименование организации |
| INN | ИНН организации |
| OGRN | ОГРН организации |
| SurName (SN) | Фамилия полномочного представителя, действующего от имени организации |
| GivenName (GN) | Имя и Отчество полномочного представителя |
| SNILS | СНИЛС полномочного представителя |

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

Приложение № 5
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на приостановление действия сертификата
ключа проверки электронной подписи)

Заявление на приостановление действия сертификата
ключа проверки электронной подписи
Оператора Удостоверяющего центра

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

| | |
|---|---|
| SerialNumber (SN) | Серийный номер сертификата ключа проверки электронной подписи |
| CommonName (CN) | Наименование организации |
| INN | ИНН организации |
| OGRN | ОГРН организации |
| SurName (SN) | Фамилия полномочного представителя, действующего от имени организации |
| GivenName (GN) | Имя и Отчество полномочного представителя |
| SNILS | СНИЛС полномочного представителя |

Срок приостановления действия сертификата ключа проверки электронной подписи _____ дней.
(количество прописью)

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

Приложение № 6
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на возобновление действия сертификата
ключа проверки электронной подписи)

Заявление на возобновление действия сертификата
ключа проверки электронной подписи
Оператора Удостоверяющего центра

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

| | |
|---|---|
| SerialNumber (SN) | Серийный номер сертификата ключа проверки электронной подписи |
| CommonName (CN) | Наименование организации |
| INN | ИНН организации |
| OGRN | ОГРН организации |
| SurName (SN) | Фамилия полномочного представителя, действующего от имени организации |
| GivenName (GN) | Имя и Отчество полномочного представителя |

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

Приложение № 7
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на получение информации о статусе сертификата ключа проверки
электронной подписи)

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО» и содержащего следующие данные:

| | |
|---|---|
| SerialNumber (SN) | Серийный номер сертификата ключа проверки электронной подписи |
| CommonName (CN) | Наименование организации, если владелец сертификата ключа проверки электронной подписи – юридическое лицо; Фамилия, Имя, Отчество, если владелец сертификата ключа проверки электронной подписи – физическое лицо |

Время[1] (период времени) на момент наступления которого требуется установить статус сертификата ключа проверки электронной подписи: с «_____» по «_____».

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

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

Приложение № 8
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на подтверждение подлинности
электронной подписи в электронном документе)

Заявление на подтверждение подлинности электронной подписи в электронном документе

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

1. Файл формата X.509, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению носителе – рег. № МД–XXX;

2. Файл, созданный с использованием Сервиса электронной подписи, содержащий подписанные ЭП данные и значение ЭП, либо файл, содержащий исходные данные и файл, содержащий значение ЭП формата CMS, на прилагаемом к заявлению носителе – рег. № МД–XXX

3. Время[2] на момент наступления которых требуется подтвердить подлинность ЭП: «_____:_____» «_____/_____/_____»;
час минута день месяц год

Оператор Удостоверяющего центра
ООО «КРИПТО-ПРО» _____/_____/

«____» _____ 20____ г.

_____ _____ /_____/
(Должность руководителя организации) (подпись) (фамилия, инициалы)

«___»_____20__ г.

М.П.

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

Приложение № 9
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма сертификата ключа проверки электронной
подписи на бумажном носителе)

## Копия сертификата ключа проверки электронной подписи

**Сведения о сертификате:**
**Кому выдан:**
ООО "Сочинские колбасы"
**Версия:** 3 (0x2)
**Серийный номер:** 61D0 B15A 0007 0000 007F
**Издатель сертификата:** CN = ООО «КРИПТО-ПРО», O = ООО "КРИПТО-ПРО", L = Москва, S = г. Москва, C = RU, E = qca@cryptopro.ru, STREET = ул. Сущёвский вал, д.16, стр.5, ИНН = 007717107991, ОГРН = 1037700085444
**Срок действия:**
Действителен с: 01 сентября 2018 г. 14:14:00 UTC
Действителен по: 01 сентября 2019 г. 14:24:00 UTC
**Владелец сертификата:** SN = Петров, G = Пётр Петрович, T = Главный администратор, STREET = Курортный пр-т, дом 98/25, CN = ООО "Сочинские колбасы", OU = Отдел по закупкам оборудования, O = ООО "Сочинские колбасы", L = Сочи, S = 23 Краснодарский край, C = RU, E = petrov@sochikolb.ru, ИНН = 002311111111, ОГРН = 1234567890777
**Ключ проверки электронной подписи:**
Алгоритм ключа проверки электронной подписи:
Название: ГОСТ Р 34.10-2012 256 бит
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 76B0 EA28 93AF B020 70E5 869B E005 80A5 8EED 9157 67FD 5225 2657 2D04 F722 6217 3D98 F03E 8E31 D430 84F8 5E7E A79A 6411 E431 D408 8033 30A9 8629 B926 6CCC DD8D
**Расширения сертификата X.509**
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: e6 5f ca b6 c0 d0 38 a1 eb ab 96 4d 1a 44 21 f9 d9 6b 0b 09
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=a4 58 57 89 36 5a 85 01 b2 90 f9 9b 44 35 f6 42 b7 99 c4 6b Поставщик сертификата: Адрес каталога: CN = ООО «КРИПТО-ПРО», O = ООО "КРИПТО-ПРО", L = Москва, S = г. Москва, C = RU, E = qca@cryptopro.ru, STREET = ул. Сущёвский вал, д.16, стр.5, ИНН = 007717107991, ОГРН = 1037700085444 Серийный номер сертификата=07 a8 f5 9a 9a 64 15 95 46 5f 24 b0 3b 71 d4 53
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://q.cryptopro.ru/ra/cdp/A4585789365A8501B290F99B4435F642B799C46B.crl
6. Расширение 2.5.29.16
Название: Период использования закрытого ключа
Значение: Действителен с 01 сентября 2018 г. 18:14:00 Действителен по 01 сентября 2019 г. 18:14:00
7. Расширение 1.2.643.100.111
Название: Средство электронной подписи владельца
Значение: Средство электронной подписи: ПАКМ «КриптоПро HSM» версия 2.0. Комплектация 3 Исполнение «DSS + myDSS»
8. Расширение 1.2.643.100.112
Название: Средства электронной подписи и УЦ издателя
Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0) Заключение на средство ЭП: Сертификат соответствия СФ/124-3010 от 30.12.2016 Средство УЦ: ПАК "КриптоПро УЦ" (версии 2.0) Заключение на средство УЦ: Сертификат соответствия № СФ/128-2983 от 18.11.2016
9. Расширение 2.5.29.32
Название: Политики сертификата
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1
**Подпись Удостоверяющего центра:**
Алгоритм подписи:
Название: ГОСТ Р 34.11-2012/34.10-2012 256 бит
Идентификатор: 1.2.643.2.2.3
Значение: 0D47 F9D8 F0EE B4FE F915 5356 DECF F1CE 1275 A4E9 5973 1D99 F177 2453 DE0E 8DA5 1F86 B62C 024D 21F0 738F 604E 1774 DB30 91C5 B52B D14B 1727 8979 C98D 94B3 C9B9

Подпись владельца сертификата/полномочного представителя: _____/_____

"___" _____ 20__ г.

Приложение № 10
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на подключение Стороннего центра идентификации)

Заявление на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подключить к Сервису электронной подписи ООО «КРИПТО-ПРО» Сторонний центр идентификации (СЦИ) в соответствии с указанными в настоящем заявлении сведениями:

| № п/п | Параметр СЭП | Настраиваемое значение параметра СЦИ | |
|---|---|---|---|
| 1. | Уникальный идентификатор СЦИ | Латинские буквы и цифры без пробелов (определяет УО) | |
| 2. | Наименование СЦИ | Отображаемое в Web-интерфейсе СЭП имя стороннего ЦИ (определяет УО) | |
| 3. | Адрес ЦИ | URL-адрес взаимодействия с ЦИ (необходим при web-доступе) | |
| 4. | Краткое описание ЦИ | Краткие сведения о подключаемом ЦИ | |
| 5. | Срок действия сертификата СЦИ | Дата начала и окончания действия сертификата Стороннего ЦИ (NotBefore, NotAfter) | |
| 6. | Отпечаток сертификата СЦИ | Хеш сертификата Стороннего ЦИ (sha1) | |
| 7. | Режим регистрации пользователей СЦИ в СЭП | Автоматический (при первичном обращении к СЭП)/Оператором СЦИ | |
| 8. | Отображаемое наименование группы пользователей (1). | Опционально. Если не указан – используется группа по умолчанию для всех пользователей.<br>Указать для всех планируемых групп в дополнительных пунктах. | |
| | | Уникальный идентификатор группы пользователей (1). | Определяет УО для каждой указанной группы. |
| 9. | ФИО | Работник Уполномоченной Организации, ответственный за подключение и функционирование ЦИ, и его контактные данные: | |
| 10. | Подразделение | Ответственного работника Уполномоченной организации | |
| 11. | Адрес электронной почты | Ответственного работника Уполномоченной организации | |
| 12. | Номер рабочего телефона | Ответственного работника Уполномоченной организации | |

К настоящему заявлению прилагаются в электронной форме:

1. Сертификат ключа проверки электронной подписи, используемый для проверки электронной подписи Стороннего центра идентификации передаваемых в СЭП маркеров доступа (в электронном виде формата x.509).

_____ _____ /_____/

«____» _____ 20____ г.

_____ _____ /_____/
(Должность руководителя организации) (подпись) (фамилия, инициалы)

«___»_____20__ г.

М.П.

Приложение № 11
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на подключение SMS-шлюза)

Заявление на подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подключить SMS-шлюз к Сервису электронной подписи ООО «КРИПТО-ПРО» в соответствии с указанными в настоящем заявлении сведениями:

| | |
|---|---|
| URL и сетевой (IP)-адрес SMS-шлюза | URL-адрес SMS-шлюза Уполномоченной организации |
| | IP-адрес и номер порта SMS-шлюза Уполномоченной организации |
| Идентификационные данные | Логин и пароль для подключения к SMS-шлюзу Уполномоченной организации |
| ФИО | Работник Уполномоченной Организации, ответственный за подключение и функционирование SMS-шлюза Уполномоченной организации, и его контактные данные: |
| Подразделение | Ответственного работника Уполномоченной Организации |
| Рабочий адрес электронной почты | Ответственного работника Уполномоченной Организации |
| Номер рабочего телефона | Ответственного работника Уполномоченной Организации |

К настоящему заявлению прилагаются в электронной форме:

1. Спецификация, содержащая технические условия подключения SMS-шлюза Уполномоченной организации.

_____ _____ /_____/

«____» _____ 20____ г.

_____ _____ /_____/
(Должность руководителя организации) (подпись) (фамилия, инициалы)

«___»_____20__ г.

М.П.

Приложение № 12
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Функции Сервиса электронной подписи)

# Реализуемые функции Сервиса электронной подписи ООО «КРИПТО-ПРО»

## 1. Назначение сервиса

Сервис электронной подписи ООО «КРИПТО-ПРО» (СЭП) предназначен для централизованного:

1. Создания и хранения ключей электронной подписи Пользователей Удостоверяющего центра.
2. Создания и проверки электронной подписи электронных документов различного формата криптографических сообщений.
3. Взаимодействия Операторов и Пользователей Удостоверяющего центра с Удостоверяющим центром для управления сертификатами ключей проверки электронной подписи.

## 2. Поддерживаемые форматы и стандарты

Электронная подпись создается с использованием криптографических алгоритмов в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Поддерживаемые форматы криптографических сообщений:

1. «Чистая» (необработанная) Электронная подпись ГОСТ 34.10 – 2001, ГОСТ 34.10 – 2012;
2. Усовершенствованная подпись в соответствии с ETSI TS 101 733 "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)", рекомендациями RFC 5652, "Cryptographic Message Syntax" (CAdES-BES и CAdES-X Long Type 1);
3. Подпись XML-документов (XML Digital Signature, XMLDSig);
4. Подпись документов PDF (Open Document Format);
5. Подпись документов Microsoft Office (Office Open XML).

## 3. Используемые средства электронной подписи

Для создания и хранения ключей электронной подписи Пользователей Удостоверяющего центра, создания электронной подписи электронных документов в составе Сервиса электронной подписи используется сертифицированное средство электронной подписи ПАКМ «КриптоПро HSM».

Для проверки электронной подписи электронных документов используется сертифицированное средство электронной подписи СКЗИ «КриптоПро CSP».

## 4. Предоставление доступа к сервису

Доступ к Сервису электронной подписи осуществляется круглосуточно в режиме 24x7 по каналам связи посредством Веб-интерфейса, предоставляемого Удостоверяющим центром, или Прикладного интерфейса, используемого для подключения Информационных систем

Уполномоченной организации в соответствии руководством разработчика программного обеспечения «КриптоПро DSS».

Аутентификация пользователей осуществляется с использованием штатного Центра идентификации в составе ПАК «КриптоПро DSS» или по протоколу SAML (WS Security) или OpenID с использованием Стороннего центра идентификации Уполномоченной организации, подключаемого к Сервису электронной подписи в соответствии с документацией на программное обеспечение «КриптоПро DSS».

Руководства доступны по адресу https://www.cryptopro.ru/products/dss/downloads.

Вторичная аутентификация пользователей осуществляется посредством ключа аутентификации в мобильном приложении (программе для ЭВМ) «КриптоПро myDSS» из состава ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» версии 2.0» на устройствах Пользователей УЦ; одноразового кода, высылаемого Пользователям УЦ в информационном сообщении или формируемого с помощью OTP-токена.

Допускается прерывание функционирования СЭП для проведения плановых регламентных работ не более чем на 1 час. В случае возникновения внештатных ситуаций восстановление функционирования СЭП осуществляется в течение 1 часа рабочего времени.

## 5. Информирование Пользователей Удостоверяющего центра

СЭП позволяет информировать Пользователей Удостоверяющего центра посредством отправки информационных сообщений, содержащих сведения о подключении к СЭП и подписываемых электронных документах от имени Пользователя Удостоверяющего центра, выполняемых операциях с ключом электронной подписи, принадлежащих Пользователю Удостоверяющего центра.

## 6. Защита информации

Защита от несанкционированного доступа ключей электронной подписи пользователей осуществляется с использованием сертифицированного средства криптографической защиты информации ПАКМ «КриптоПро HSM».

Защита информации, передаваемой при подключении Информационной системы, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра.

Защита аутентификационной информации, передаваемой при подключении Стороннего центра идентификации, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра.

Защита информации, передаваемой при подключении SMS-шлюза, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра.

Обеспечение информационной безопасности подтверждается аттестатом соответствия объекта информатизации автоматизированной системы Сервиса электронной подписи требованиям по защите информации от несанкционированного доступа.

## 7. Правила пользования Сервисом электронной подписи

Ключи электронной подписи формируются в СЭП в неэкспортируемом формате, т.е. недоступном для сохранения и использования на съемных ключевых носителях и рабочем месте пользователя.

При создании ключа электронной подписи в СЭП Пользователем Удостоверяющего центра может быть установлен индивидуальный PIN-код доступа к ключевому контейнеру, содержащему ключ электронной подписи.

Создание сертификата ключа проверки электронной подписи для использования в СЭП осуществляться подключенным к СЭП Удостоверяющим центром.

Использование ключа электронной подписи в СЭП должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем УЦ) с помощью ключа аутентификации в мобильном приложении (программе для ЭВМ) «КриптоПро myDSS» на устройстве Пользователя УЦ; или одноразового пароля, формируемого персональным OTP-токеном владельца сертификата ключа проверки электронной подписи или высылаемого в информационном сообщении на указанный при регистрации Пользователем УЦ мобильный телефон владельца сертификата ключа электронной подписи Пользователя УЦ, а также (опционально) индивидуальным PIN-кодом доступа к ключевому контейнеру, содержащему используемый ключ электронной подписи.

Пользователь Удостоверяющего центра должен хранить в тайне индивидуальный PIN-код доступа к ключевому контейнеру, аутентификационную информацию, обеспечить сохранность персональных средств аутентификации (ключ аутентификации для мобильного приложения (программы для ЭВМ) «КриптоПро myDSS», OTP-токен, мобильный телефон и SIM-карту для получения одноразового пароля), используемые для подтверждения использования ключа электронной подписи для подписания электронного документа, принимать все возможные меры для предотвращения их потери, раскрытия и несанкционированного использования.

Пользователь Удостоверяющего центра обязан немедленно обратиться к Оператору Удостоверяющего центра с заявлением на приостановление действия или прекращение действия соответствующего сертификата ключа проверки электронной подписи в случае раскрытия, искажения персонального ключа электронной подписи, компрометации аутентификационной информации и утери специальных устройств, используемых для аутентификации (ключа аутентификации для мобильного приложения (программы для ЭВМ) «КриптоПро myDSS», мобильного телефона, SIM-карты и (или) OTP-токена), а также в случае, если Пользователю Удостоверяющего центра стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе если Пользователь УЦ получил сообщение от СЭП о выполнении каких-либо операций от его имени в то время, когда он их не выполнял.

На рабочих местах Пользователей Удостоверяющего центра должны использоваться сертифицированные средства антивирусной защиты в соответствии с эксплуатационной документацией.

## 8. Аудит Сервиса электронной подписи

Регистрация всех операций, выполняемых Операторами и Пользователями Удостоверяющего центра, осуществляется средствами СЭП. Журналы аудита выгружаются средствами СЭП и используются для контроля и анализа выполненных операций при разборе спорных вопросов и разрешении конфликтных ситуаций. Оператор УЦ доступ к журналу аудита имеет посредством Веб-интерфейса, предоставляемого Удостоверяющим центром.

Приложение № 13
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма перечня параметров функционирования СЭП для настройки доступа Операторов и Пользователей УЦ)

Перечень параметров функционирования Сервиса электронной подписи ООО «КРИПТО-ПРО» для настройки доступа Операторов и Пользователей УЦ

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Подтверждает подключение к Сервису электронной подписи ООО «КРИПТО-ПРО» в соответствии с указанными значениями параметров функционирования (целевые значения параметров необходимо отмечать символом «+»; **первоначально отмечены символом «+» значения по умолчанию**) экземпляра СЭП:

| № п/п | Параметр СЭП | Настраиваемое значение параметра СЭП | |
|---|---|---|---|
| **Адреса веб-интерфейсов СЭП** | | | |
| 1. | URL-адрес веб-интерфейса сервиса подписи[3] | *Выбрать из списка (одно):* | |
| | | + | https://saas.cryptopro.ru/INSTANCE/<br>*Порты доступа TLS*: 443 (RSA), 4430 (ГОСТ) |
| | | | «Не предоставлять» |
| 2. | URL-адрес личного кабинета Пользователей СЭП | *Выбрать из списка (одно):* | |
| | | + | https://saas.cryptopro.ru/INSTANCEidp/users/<br>*Порты доступа TLS*: 443 (RSA), 4430 (ГОСТ) |
| | | | «Не предоставлять» |
| 3. | URL-адрес веб-интерфейса для подключения Оператора СЭП | *Выбрать из списка (одно):* | |
| | | + | https://saas.cryptopro.ru/INSTANCEidp/admins/<br>*Порты доступа TLS*: 443 (RSA), 4430 (ГОСТ) |
| | | | «Не предоставлять» |
| **Адреса программных интерфейсов СЭП** | | | |
| 4. | Базовый URL-адрес Прикладного интерфейса СЭП | SOAP: https://saas.cryptopro.ru/INSTANCEss/<br>REST: https://saas.cryptopro.ru/INSTANCEss/rest/api<br>*Порт доступа (алгоритм шифрования трафика (TLS))*: 443 (RSA) | |
| 5. | Базовый URL-адрес Центра идентификации СЭП | https://saas.cryptopro.ru/INSTANCEidp<br>https://saas.cryptopro.ru/INSTANCEidp/ums/<br>*OAuth 2.0*:<br>https://saas.cryptopro.ru/INSTANCEidp/oauth/authorize<br>https://saas.cryptopro.ru/INSTANCEidp/oauth/token | |

[3] Имя экземпляра СЭП **INSTANCE** должно состоять только из строчных (нижний регистр) латинских букв и цифр и не должно начинаться с цифры. Чаще всего **INSTANCE** выбирают равным доменному имени Организации без зонального суффикса (для ООО «КРИПТО-ПРО» (домен cryptopro.ru) **INSTANCE** в этом случае был бы равен **cryptopro**)

<table>
<tr><td></td><td></td><td colspan="3">Порт доступа (алгоритм шифрования трафика (TLS)): 443 (RSA)</td></tr>
<tr><td>6.</td><td>URL-адрес сервиса проверки ЭП</td><td colspan="3">https://saas.cryptopro.ru/verifyqca - для СЭП Аккредитованного УЦ</td></tr>
<tr><td rowspan="2">7.</td><td rowspan="2">Сетевые адреса (IP) СЭП</td><td colspan="3">Входящий: 193.37.157.28</td></tr>
<tr><td colspan="3">Исходящий: 193.37.157.5</td></tr>
<tr><td rowspan="2">8.</td><td rowspan="2">Сетевые адреса (IP) Источника запросов к СЭП[4]</td><td colspan="3">Указать IP-адрес, или диапазон IP-адресов:</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="5">Настройки СЭП</td></tr>
<tr><td rowspan="6">9.</td><td rowspan="6">Доступные форматы подписи</td><td colspan="3">Выбрать из списка (одно, или несколько):</td></tr>
<tr><td>+</td><td colspan="2">«Чистая» ЭП ГОСТ Р 34.10-2012</td></tr>
<tr><td>+</td><td colspan="2">CAdES-BES/T/X Long Type 1</td></tr>
<tr><td>+</td><td colspan="2">XMLDSig</td></tr>
<tr><td>+</td><td colspan="2">PDF-CMS/CAdES</td></tr>
<tr><td>+</td><td colspan="2">Microsoft Office</td></tr>
<tr><td rowspan="4">10.</td><td rowspan="4">Использование PIN-кода для ключевого контейнера</td><td colspan="3">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td colspan="2">«Позволять задавать»</td></tr>
<tr><td></td><td colspan="2">«Требовать»</td></tr>
<tr><td></td><td colspan="2">«Не требовать»</td></tr>
<tr><td>11.</td><td>Максимальный размер подписываемого документа (до 50 МБ)</td><td colspan="3">5 МБ</td></tr>
<tr><td>12.</td><td>URL-адрес Службы штампов времени (TSP)</td><td colspan="3">http://qs.cryptopro.ru/tsp/tsp.srf<br>для СЭП Аккредитованного УЦ ООО «КРИПТО-ПРО»</td></tr>
<tr><td colspan="5">Настройки Центра идентификации СЭП</td></tr>
<tr><td>13.</td><td>Отпечаток сертификата (значение хеша sha1) Центра идентификации СЭП</td><td colspan="3">Заполняется только при использовании стороннего Центра идентификации СЭП[5]</td></tr>
<tr><td rowspan="3">14.</td><td rowspan="3">Режим создания учетных записей в СЭП для пользователей сторонних Центров идентификации</td><td colspan="3">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td colspan="2">«Автоматически при первой аутентификации пользователя к СЭП»</td></tr>
<tr><td></td><td colspan="2">«Вручную Оператором СЭП»</td></tr>
<tr><td colspan="5">Профиль Пользователя</td></tr>
<tr><td rowspan="4">15.</td><td rowspan="4">Состав компонентов имени (RDN) Пользователя</td><td colspan="3">Выбрать из списка (одно, или несколько); при необходимости указать значения по умолчанию для выбранных RDN:</td></tr>
<tr><td>RDN</td><td>Обязательно для заполнения</td><td>Значение по умолчанию</td></tr>
<tr><td>ОГРН</td><td></td><td></td></tr>
<tr><td>ОГРНИП</td><td></td><td></td></tr>
<tr><td>СНИЛС</td><td></td><td></td></tr>
</table>

[4] Указать IP-адреса (диапазон IP-адресов) серверов прикладной системы (приложения) Заказчика, которые будут обращаться к СЭП

[5] Сертификат стороннего Центра идентификации нужно передать в ООО «КРИПТО-ПРО» для создания экземпляра со сторонним Центром идентификации

| | | | | |
|---|---|---|---|---|
| | | ИНН | | |
| | | Электронная почта | | |
| | | Страна | + | RU |
| | | Область | | |
| | | Город | + | |
| | | Организация | + | |
| | | Подразделение | | |
| | | Общее имя | + | |
| | | Адрес | | |
| | | Должность | | |
| | | Инициалы | | |
| | | Имя | + | |
| | | Фамилия | + | |

| | | | |
|---|---|---|---|
| 16. | Самостоятельное редактирование профиля Пользователем | *Выбрать из списка (одно):* | |
| | | + | «Запретить» |
| | | | «Разрешить» |
| **Политика учетных записей Пользователей** | | | |
| 17. | Используемые идентификаторы Пользователя[6] | *Выбрать из списка ниже (одно, или несколько):* | |
| | | + | Логин |
| | | | Номер телефона |
| | | | Адрес электронной почты (e-mail) |
| 18. | Подтверждение номера телефона Пользователя отправкой SMS[7] | *Выбрать из списка (одно):* | |
| | | + | «Не требуется» |
| | | | «Требуется» |
| 19. | Подтверждение e-mail Пользователя отправкой электронного письма[8] | *Выбрать из списка (одно):* | |
| | | + | «Не требуется» |
| | | | «Требуется» |
| 20. | Самостоятельная регистрация Пользователей в СЭП | *Выбрать из списка (одно):* | |
| | | + | «Запрещена» |
| | | | «Разрешена» |
| 21. | Временная блокировка самостоятельно | *Выбрать из списка (одно):* | |
| | | + | «Нет» |

[6] При этом выбранные идентификаторы должны быть уникальны для каждого Пользователя

[7] Заполняется только если в числе идентификаторов Пользователя выбран номер телефона

[8] Заполняется только если в числе идентификаторов Пользователя выбран адрес электронной почты (e-mail)

| | | | |
|---|---|---|---|
| | зарегистрировавшихся Пользователей в СЭП[9] | | «Да» |
| **Настройки первичной аутентификации Пользователей** | | | |
| 22. | Виды первичной аутентификации Пользователей | *Выбрать из списка ниже (одно):* | |
| | | | Только идентификация |
| | | + | По паролю/сертификату |
| 23. | Разрешить Пользователям самостоятельное изменение настроек первичной аутентификации | *Выбрать из списка (одно):* | |
| | | + | «Нет» |
| | | | «Да» |
| **Политики парольной аутентификации** | | | |
| 24. | Длина долговременных паролей (*от 1 до 256 символов*) | 8 символов | |
| 25. | Сложность долговременных паролей | *Выбрать из списка (одно):* | |
| | | + | «Цифры и буквы в разном регистре» |
| | | | «Цифры и буквы в разном регистре и специальные символы» |
| | | | «Цифры и буквы» |
| | | | «Только цифры» |
| 26. | Максимальное количество попыток ввода долговременного пароля до блокирования учётной записи (*от 0 до 2147483647*) | *Выбрать из списка (одно):* | |
| | | + | «5» (можно указать собственное значение) |
| | | | «0» (Блокирование отключено) |
| 27. | Срок действия долговременного пароля (*в днях*) | *Выбрать из списка (одно):* | |
| | | + | Срок действия не ограничен |
| | | | «Указать количество дней» |
| 28. | Требовать смену пароля Пользователя при первом входе в СЭП[10] | *Выбрать из списка (одно):* | |
| | | + | «Не требовать» |
| | | | «Требовать» |
| **Политики вторичной аутентификации** | | | |
| 29. | Метод вторичной аутентификации по умолчанию | *Выбрать из списка (одно):* | |
| | | + | myDSS |
| | | | OTP-SMS |
| | | | OTP-EMAIL |

[9] Заполняется только если самостоятельная регистрация Пользователей в СЭП разрешена

[10] Применяется только для учетных записей Пользователей, созданных Оператором СЭП, или в случае если пароль Пользователя был сброшен Оператором СЭП

| | | | |
|---|---|---|---|
| | | | OTP-TOKEN |
| 30. | Список операций, требующих подтверждения[11] | *Выбрать из списка ниже (одно, или несколько):* | |
| | | + | Подпись документа |
| | | + | Подпись пакета документов |
| | | + | Расшифрование документа |
| | | + | Создание запроса на сертификат |
| | | + | Удаление сертификата |
| | | + | Смена PIN-кода для доступа к закрытому ключу сертификата |
| | | + | Создание запроса на обновление сертификата |
| | | + | Создание запроса на отзыв сертификата |
| | | + | Создание запроса на приостановление действия сертификата |
| | | + | Возобновление действия сертификата |
| | | | Выпуск маркера безопасности («вход» Пользователя) |
| 31. | Разрешить Пользователям самостоятельное изменение настроек вторичной аутентификации | *Выбрать из списка (одно):* | |
| | | + | «Нет» |
| | | | «Да» |
| 32. | Разрешить Операторам изменение настроек вторичной аутентификации Пользователей | *Выбрать из списка (одно):* | |
| | | + | «Нет» |
| | | | «Да» |
| **Политика одноразовых паролей** | | | |
| 33. | Длина одноразовых паролей (*от 1 до 256 символов*) | 7 символов | |
| 34. | Сложность одноразовых паролей | *Выбрать из списка (одно):* | |
| | | | «Только цифры» |
| | | | «Цифры и буквы» |
| | | + | «Цифры и буквы в разном регистре» |
| | | | «Цифры и буквы в разном регистре и специальные символы» |
| 35. | Максимальное количество попыток ввода одноразового пароля до блокирования учётной записи (от 0 до 2147483647) | *Выбрать из списка (одно):* | |
| | | + | «5» (можно указать собственное значение) |
| | | | «0» (Блокирование отключено) |
| 36. | Время жизни транзакции в секундах | «300» (можно указать собственное значение) | |

[11] Заполняется только если вторичная аутентификация настраивается Оператором СЭП по списку операций

| | | | |
|---|---|---|---|
| 37. | Минимальное время в секундах, в течение которого Пользователь не сможет запрашивать повторную аутентификацию транзакции[12] | «0» (можно указать собственное значение) | |
| 38. | Доставлять ключ myDSS двумя частями[13] | *Выбрать из списка (одно):* | |
| | | + | «Требуется» |
| | | | «Не требуется» |
| **Группы Пользователей СЭП** | | | |
| 39. | Информация о группах пользователей и их Операторах | *Выбрать из списка (одно):* | |
| | | + | «Группа пользователей по умолчанию» |
| | | | «Собственные группы пользователей» (указать в таблице ниже) |
| | | *Имя группы* | *Описание группы* / *Логин Оператора группы* |
| | | | |
| | | | |
| | | | |
| 40. | Политика подтверждения операций для групп Пользователей[14] | *Выбрать из списка (одно):* | |
| | | + | «Соответствует политикам Центра идентификации» |
| | | | «Назначается для группы» |
| **Взаимодействие с УЦ** | | | |
| 41. | Наименование УЦ | Аккредитованный УЦ ООО «КРИПТО-ПРО» | |
| 42. | Автоматическое создание сертификатов по запросу Пользователей | *Выбрать из списка (одно):* | |
| | | + | «Запрещено» |
| | | | «Разрешено» |
| 43. | Автоматическое управление и обновление сертификатов по запросу Пользователей СЭП[15] | *Выбрать из списка (одно):* | |
| | | + | «Запрещено» |
| | | | «Разрешено» |
| **Настройки уведомлений** | | | |
| 44. | Перечень событий для рассылки уведомлений Пользователям и Операторам | *Выбрать значения уведомлений Операторов и Пользователей СЭП во вложенной таблице:*  Уведомления_СЭП.xlsx | |
| 45. | Перечень адресов электронной почты и | *Указать адреса E-Mail и (или) номера мобильных телефонов Операторов СЭП[16]:* | |

[12] При значении «0» можно создавать множество одновременных транзакций
[13] Использовать дополнительный код активации по SMS или e-mail
[14] Если используется разделение Пользователей на группы
[15] При наличии действующих сертификатов у Пользователей СЭП
[16] Если в таблице уведомлений СЭП из пункта 44 в разделе «Оповещение операторов» включено уведомление хотя бы об одном событии СЭП с использованием способов доставки E-Mail/SMS

| | | |
|---|---|---|
| | номеров мобильных телефонов для рассылки уведомлений Операторам о событиях СЭП | |
| | | |
| | | |
| | | |
| | | |
| | | |
| **Параметры OAuth** | | |
| 46. | Адрес перенаправления redirect_uri | *Заполняется после создания экземпляра СЭП* |
| 47. | Идентификатор клиента client_id | *Заполняется после создания экземпляра СЭП* |

:

_____ _____ /_____/

«____» _____ 20____ г.

_____ _____ /_____/
(Должность руководителя организации) (подпись) (фамилия, инициалы)

«___»_____20__ г.

М.П.

Приложение № 14
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на регистрацию Оператора Стороннего центра идентификации)

Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит зарегистрировать в Сервисе электронной подписи ООО «КРИПТО-ПРО» Оператора Стороннего центра идентификации (СЦИ) в соответствии с указанными в настоящем заявлении сведениями:

| | |
|---|---|
| Уникальный идентификатор СЦИ | Латинские буквы и цифры без пробелов в соответствии с заявлением на подключение Стороннего ЦИ к СЭП |
| Уникальный идентификатор и отображаемое имя группы пользователей в СЦИ | Для всех групп, пользователями которых должен управлять оператор. |
| Уникальное имя (логин) Оператора в СЦИ | Латинские буквы и цифры без пробелов |
| ФИО | Работника Уполномоченной организации, назначенный Оператором СЦИ, и его контактные данные: |
| Подразделение | Ответственного работника Уполномоченной организации |
| Адрес электронной почты | Ответственного работника Уполномоченной организации |
| Номер рабочего телефона | Ответственного работника Уполномоченной организации |

Прошу использовать адрес электронной почты _____ и (или) номер мобильного телефона для отправки почтовых сообщений и SMS-сообщений через оператора сотовой связи с уведомлением о событиях Сервиса электронной подписи

_____
*Код страны, код региона, номер телефона в формате +X-XXX-XXX-XX-XX*

*(указывается при необходимости такой рассылки)*

Настоящим _____
(фамилия, имя, отчество Оператора СЦИ)

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

соглашается с обработкой своих персональных данных ООО «КРИПТО-ПРО» и признает, что персональные данные, а именно: фамилия, имя, отчество; подразделение Уполномоченной организации, адрес электронной почты; номер телефона, ООО «КРИПТО-ПРО» имеет право обрабатывать следующими способами: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных. Настоящее согласие на обработку своих персональных данных ООО «КРИПТО-ПРО» дано на срок регистрации в Сервисе электронной подписи ООО «КРИПТО-ПРО», а также на 5 (пять) лет после прекращения регистрации в Сервисе электронной подписи ООО «КРИПТО-ПРО». Настоящим также согласен с получением на вышеуказанный номер

мобильного телефона и адрес электронной почты информационных сообщений, одноразовых паролей и уведомлений о выполняемых операциях с использованием выпущенного ключа электронной подписи.

_____ _____ /_____/
«____» _____ 20____ г.

_____ _____ /_____/
(Должность руководителя организации) (подпись) (фамилия, инициалы)
«___»_____20__ г.

М.П.

Приложение № 15
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма доверенности Оператора Стороннего центра идентификации)

Доверенность

г. _____ «_____» _____20___ г.

_____
(полное наименование Уполномоченной 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)

действовать от имени _____
(полное наименование организации)

при использовании электронной подписи электронных документов, выступать в роли Оператора Стороннего центра идентификации и осуществлять действия по обеспечению создания и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, зарегистрированных в том же Стороннем центре идентификации Уполномоченной организации.

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

Подпись Оператора Стороннего центра идентификации

_____ _____
(Фамилия И.О.) (Подпись)

подтверждаю.

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