Утвержден
Приказом ООО «КРИПТО-ПРО»
от «03» сентября 2015 г. № 32

РЕГЛАМЕНТ

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

Редакция № 1

г. Москва
2015

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 регистрации № 001.602.749 выдано 16.11.1999 г. Государственным учреждением Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003 г.).

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению неквалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий, опубликованных в сети Интернет по адресу: https://www.cryptopro.ru/about/licenses.

Реквизиты ООО «КРИПТО-ПРО»:

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

Юридический адрес: 105318, г. Москва, ул. Ибрагимова, д. 31, офис 30Б

Адрес для корреспонденции: 127018, г. Москва, ул. Сущевский вал, д. 18, А/Я «КРИПТО-ПРО»

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

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

ИНН/КПП: 7717107991/771901001

ОГРН: 1037700085444

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

Код по ОКПО: 51282566

Контактные телефоны, факс, адрес электронной почты:

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

Адрес в сети Интернет: http://cpca.cryptopro.ru

2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Договором, 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, аннулирование, 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.

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.

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

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 – 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.

Оператор Удостоверяющего центра (Оператор УЦ) – физическое лицо, действующее от имени Уполномоченной организации по обеспечению создания, выдачи и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра.

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

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец ключа проверки электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи.

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 по протоколу SOAP в соответствии с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика» и защищенный с

использованием сертифицированных 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 Удостоверяющего центра (Регламент) - настоящий документ Удостоверяющего центра, отражающий права и обязанности членов группы администраторов Удостоверяющего центра и Уполномоченной Организации, протоколы работы, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования Удостоверяющего центра и предоставления Сервиса электронной подписи.

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 изготовление 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.

Сервис электронной подписи (СЭП) - комплекс организационных, технических и программных средств Удостоверяющего центра, обеспечивающих для Пользователей Удостоверяющего центра удаленную реализацию функций централизованного хранения ключей электронной подписи, создания и проверки усиленной неквалифицированной 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 - неквалифицированный сертификат ключа проверки электронной подписи, являющийся электронным документом, созданным Удостоверяющим центром, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;
- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован, 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.

Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра (Сертификат Пользователя УЦ) - сертификат ключа проверки электронной подписи, ключ электронной подписи которого 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, выданных Удостоверяющим центром.

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

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

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

Список отозванных сертификатов (СОС) – электронный документ с неквалифицированной 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 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 2.0 в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» и используемая Уполномоченной Организацией для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи.

Тестовый сертификат – временный сертификат ключа проверки электронной подписи, 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

неквалифицированными 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 усиленной неквалифицированной электронной подписи.

Уполномоченная организация – юридическое лицо, заключившее с Удостоверяющим центром договор, наделяющий данное юридическое лицо полномочиями по обеспечению создания, выдачи и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра для предоставления доступа к Сервису электронной подписи.

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

Электронная подпись (ЭП) – усиленная неквалифицированная 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 открытого ключа, 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 документом

«ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» и используемая Уполномоченной Организацией для отправки Пользователям Удостоверяющего центра одноразовых паролей и уведомлений о выполняемых операциях.

3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент Удостоверяющего центра ООО «КРИПТО-ПРО» (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://cpca.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://cpca.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 предоставляет Стороне, присоединившейся к Регламенту по ее требованию:

4.1.1. Копию лицензии ФСБ России 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), выданную Удостоверяющему центру.

4.2. 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;
- заверенные копии учредительных документов Уполномоченной организации;
- заверенную копию свидетельства о внесении записи о юридическом лице в Единый государственный реестр юридических лиц;
- 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.

4.3. Присоединяясь к настоящему Регламенту, Уполномоченная организация в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» поручает Удостоверяющему центру в лице их уполномоченных работников и иных лиц, привлекаемых Удостоверяющим центром, совершать с персональными данными, содержащимися в документах, представленных Уполномоченной организацией Удостоверяющему центру для присоединения к настоящему Регламенту, а также в документах, которые будут представлены Уполномоченной организацией Удостоверяющему центру в соответствии с 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 присоединения Уполномоченной организации к Регламенту, доступа к СЭП, в целях исполнения Регламента, реализации вытекающих из Регламента прав и обязанностей, а также в целях осуществления

Удостоверяющим центром функций, возложенных законодательством Российской Федерации.

Присоединяясь к настоящему Регламенту, 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 им 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 Регламентом с согласия субъектов персональных данных, чьи персональные данные содержатся в таких документах. 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.

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

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

5.1.6. Обеспечить уникальность идентификационных данных Операторов 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 сертификата в соответствии с порядком, определенным в настоящем Регламенте.

5.1.8. Предоставить аутентифицированным Пользователям Удостоверяющего центра, получившим сертификат ключа проверки электронной подписи, доступ к СЭП и обеспечить круглосуточное функционирование СЭП в режиме 24x7 в соответствии с настоящим Регламентом. 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 17.

5.1.9. Использовать в составе СЭП сертифицированные средства криптографической защиты информации 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 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 настоящем Регламенте.

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

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

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

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

5.1.19. Предоставить Уполномоченной организации на уточнение и согласование перечень параметров функционирования СЭП для настройки доступа Операторов и Пользователей УЦ по форме в соответствии с Приложением № 18.

5.1.20. Предоставить Уполномоченной организации необходимые права для осуществления регистрации пользователей в Удостоверяющем центре, формирования и отправки в Удостоверяющий центр заявок в электронной форме на создание и управление сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.1.21. Предоставить Уполномоченной организации необходимые права для:

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

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

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

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

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

5.1.22. Зарегистрировать в СЭП Оператора подключенного Стороннего центра идентификации Уполномоченной организации в соответствии с заявлением по форме Приложения № 19, полученного от Уполномоченной организации.

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

5.1.24. В случае отсутствия подключения к СЭП SMS-шлюза Уполномоченной организации осуществлять информирование и аутентификацию 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 выполняется эмуляция отправки информационных сообщений на номер мобильного телефона путем записи их в файл и передачи файла по запросу Уполномоченной организации.

5.1.25. 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 версию документ «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика». Информирование осуществляется путем публикации новости на сайте Удостоверяющего центра по адресу: https://www.cryptopro.ru/news.

5.2. Уполномоченная организация обязана:

5.2.1. С целью обеспечения гарантированного ознакомления Уполномоченной организации с полным текстом изменений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу: http://cpca.cryptopro.ru/reglament/reglamentoperdss.pdf - за сведениями об изменениях в Регламенте.

5.2.2. Известить Удостоверяющий центр об изменениях реквизитов Уполномоченной организации и по требованию Удостоверяющего Центра предоставить соответствующие подтверждающие документы в течение 5 (пяти) рабочих дней с момента регистрации изменений.

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

5.2.4. После проведения проверки с использованием тестовых сертификатов согласовать и подписать предоставленный Удостоверяющим центром уточненный перечень настроенных параметров функционирования СЭП для доступа Операторов и Пользователей УЦ по форме в соответствии с Приложением № 18.

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

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

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

5.2.8. 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 Пользователям Удостоверяющего центра ключей электронной подписи в соответствии с настоящим Регламентом.

5.2.9. 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.

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

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

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. Использовать для создания и проверки усиленных неквалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи 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 сертификата ключа проверки электронной подписи.

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. 4.2 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 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.

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

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

5.3.7. Отказать в создании и управлении сертификатами ключей проверки электронной подписи по заявкам Оператора УЦ до получения от Уполномоченной Организации подписанного перечня параметров функционирования СЭП для настройки прав доступа Операторов и Пользователей УЦ по форме в соответствии с Приложением № 18.

5.3.8. Отказать в подключении Стороннего центра идентификации Уполномоченной организации в случае ненадлежащего оформления заявления на подключение Стороннего центра идентификации в соответствии с Приложением № 15.

5.3.9. Отказать в подключении SMS-шлюза Уполномоченной организации в случае ненадлежащего оформления заявления на подключение SMS-шлюза в соответствии с Приложением № 16.

5.3.10. Отказать в регистрации Оператора Стороннего центра идентификации до получения надлежащим образом (в соответствии с Приложением № 15) оформленного заявления на подключение Стороннего центра идентификации Уполномоченной организации или в случае ненадлежащего оформления заявления на регистрацию Оператора СЦИ в соответствии с Приложением № 19.

5.3.11. Отказать в предоставлении доступа к СЭП Пользователям Удостоверяющего центра, не прошедшим аутентификацию и не подтвердившим выполнение операций с использованием одноразового пароля.

5.4. Уполномоченная организация имеет право:

5.4.1. Заверять печатью Уполномоченной организации копии сертификатов ключей проверки электронной подписи, решение по созданию которых было принято Оператором Удостоверяющего центра, являющимся полномочным лицом Уполномоченной организации.

5.4.2. Осуществлять с использованием Прикладного интерфейса, предоставляемого Удостоверяющим центром, подключение собственных Информационных систем к СЭП для получения доступа к функциям создания и проверки электронной подписи, управления сертификатами ключей проверки электронной подписи, хранения ключей электронной подписи Пользователей Удостоверяющего центра.

5.4.3. Осуществлять в соответствии с п.8.9 настоящего Регламента подключение к СЭП собственных Сторонних центров идентификации для управления доступом Операторов и Пользователей Удостоверяющего центра к СЭП.

5.4.4. Подать в Удостоверяющий центр заявление по форме в соответствии с Приложением № 19 на регистрацию в СЭП Оператора Стороннего центра идентификации Уполномоченной организации.

5.4.5. Осуществить в соответствии с п.8.10 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.

5.4.6. Предоставлять Пользователям УЦ совместимые со средствами Удостоверяющего центра OTP-токены для 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 УЦ право подачи заявки в УЦ на создание управление своими сертификатами ключей проверки электронной подписи посредством Веб- или Прикладного интерфейса СЭП, предоставляемых Удостоверяющим центром. Предоставленные Уполномоченной организацией права Пользователей УЦ определяются параметрами функционирования СЭП в соответствии с Приложением № 18 и Регламентом деятельности Уполномоченной организации. Уполномоченная организация несет всю полноту своих обязанностей и ответственности за создаваемые Удостоверяющим центром сертификаты по заявкам Пользователей УЦ 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 по созданию и выдаче сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.4.10.4. Прекращать, приостанавливать и возобновлять действие сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, решение по созданию которых было принято Оператором 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 УЦ 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 по занесению данных 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 копий сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра полностью возлагается на Уполномоченную организацию.

6.6. 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.

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

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

6.9. 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. Регистрация Оператора Удостоверяющего центра

Регистрация Оператора Удостоверяющего центра осуществляется на основании заявления на регистрацию Оператора Удостоверяющего центра и доверенности Оператора Удостоверяющего центра. Форма заявления на регистрацию Оператора Удостоверяющего центра приведена в Приложении № 2 настоящего Регламента, форма доверенности Оператора Удостоверяющего центра приведена в Приложении № 3 Регламента.

Предоставление заявительных документов для регистрации Оператора Удостоверяющего центра может быть осуществлено:

- Оператором Удостоверяющего центра;
- Представителем Уполномоченной организации на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра, оформленной по форме Приложения № 4 к настоящему Регламенту.

После осуществления регистрации Оператора Удостоверяющего центра Удостоверяющий центр сообщает Оператору секретную ключевую фразу и предоставляет:

- URL адреса доступа к дистрибутиву средства электронной подписи;
- URL адреса подключения к Удостоверяющему центру для получения сертификата Оператора Удостоверяющего центра;
- URL адреса подключения к Сервису электронной подписи для Оператора Удостоверяющего центра и Пользователей Удостоверяющего центра;
- Файл сертификата ключа проверки электронной подписи (корневого сертификата) Удостоверяющего центра.

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

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

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

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

1. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с генерацией ключей в Удостоверяющем центре;
2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с генерацией ключей на рабочем месте Оператора.

Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с генерацией ключей на рабочем месте Оператора может быть реализовано двумя способами:

1. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра на основании файла запроса;
2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра посредством веб-интерфейса, предоставляемого Удостоверяющим центром.

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

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

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

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

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

8.2.2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с генерацией ключей на рабочем месте Оператора на основании файла запроса

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

Для формирования запроса на сертификат Оператор Удостоверяющего центра может использовать html-файл, получаемый от Администратора Удостоверяющего центра, или иное специальное ПО, совместимое со средствами электронной подписи и Удостоверяющего центра.

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

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

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

Администратор Удостоверяющего центра осуществляет сравнение содержимого полученного по электронной почте файла запроса на сертификат с текстом запроса на

сертификат, содержащимся в заявлении на создание сертификата ключа проверки электронной подписи Оператора на бумажном носителе.

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

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

Администратор Удостоверяющего центра уведомляет сообщением по электронной почте Оператора о создании сертификата ключа проверки электронной подписи, а также в виде вложения этого сообщения направляет ему файл, содержащий созданный сертификат ключа проверки электронной подписи.

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

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

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

8.2.3. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра с генерацией ключей на рабочем месте Оператора Удостоверяющего центра посредством веб-интерфейса, предоставляемого Удостоверяющим центром

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

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

Предоставление заявления на создание сертификата ключа проверки электронной подписи Оператора УЦ на бумажном носителе осуществляется посредством почтовой или курьерской связи.

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

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

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

Администратор Удостоверяющего центра уведомляет сообщением по электронной почте Оператора УЦ о создании сертификата ключа проверки электронной подписи. После получения указанного сообщения Оператор УЦ посредством веб-интерфейса Удостоверяющего центра производит установку созданного сертификата ключа проверки электронной подписи на своем рабочем месте.

Создание сертификата ключа проверки электронной подписи и уведомление Оператора УЦ о создании сертификата должны быть осуществлены не позднее 5-ти рабочих дней, следующих за рабочим днем, в течение которого было принято заявление на создание сертификата.

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

После подтверждения получения Удостоверяющим центром завизированной Оператором УЦ копии сертификата ключа проверки электронной подписи на бумажном носителе и регистрации Администратором Удостоверяющего центра полученного сертификата в СЭП, Оператор приступает к выполнению возложенных на него обязанностей.

8.3. Плановая смена ключей Оператора Удостоверяющего центра

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

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

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

Новый сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра может быть создан на основании файла запроса аналогично п.п.8.2.2 Регламента или посредством веб-интерфейса, предоставляемого Удостоверяющим центром аналогично п.п.8.2.3. В этом случае заявление на создание сертификата подписывается только в электронной форме и доступ к веб-интерфейсу Удостоверяющего центра осуществляется на действующем ключе электронной подписи Оператора Удостоверяющего центра.

Администратор Удостоверяющего Центра на основании поступившего заявления на создание сертификата ключа проверки электронной подписи создает сертификат ключа проверки электронной подписи Оператора УЦ и распечатывает по форме Приложения № 14 два экземпляра сертификата ключа проверки электронной подписи на бумажном носителе.

Два экземпляра сертификата ключа проверки электронной подписи Оператора УЦ на бумажном носителе визируются уполномоченным на это лицом Удостоверяющего центра,

заверяются печатью Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются Оператору Удостоверяющего центра.

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

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

После подтверждения получения Удостоверяющим центром завизированного Оператором УЦ сертификата ключа проверки электронной подписи на бумажном носителе и регистрации Администратором Удостоверяющего центра полученного сертификата в СЭП, Оператор УЦ может использовать для выполнения возложенных на него обязанностей новый сертификат ключа проверки электронной подписи и соответствующий ему ключ электронной подписи.

8.4. Внеплановая смена ключей Оператора Удостоверяющего центра

Внеплановая смена ключей осуществляется Оператором Удостоверяющего центра в следующих случаях:

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

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

8.5. 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;
- в случае отзыва доверенности Оператора Удостоверяющего центра;
- по истечении срока, на который действие сертификата было приостановлено;
- по заявлению владельца сертификата ключа проверки электронной подписи;
- по истечении срока действия сертификата ключа проверки электронной подписи;
- в связи с аннулированием сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи.

В случае прекращения действия настоящего Регламента, отзыва доверенности Оператора УЦ, истечения срока, на который действие сертификата ключа проверки электронной подписи было приостановлено, прекращения действия сертификата Оператора по его заявлению, по решению суда, вступившего в законную силу, и т.д. Удостоверяющий центр должен официально уведомить Оператора УЦ и всех лиц, зарегистрированных в

Удостоверяющем центре, о прекращении действия сертификата 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, содержащего сведения об аннулированном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные 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 Оператора Удостоверяющего центра по истечении срока его действия временем прекращения действия (аннулирования) сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра признается время, хранящееся в поле notAfter поля Validity сертификата ключа проверки электронной подписи. В данном случае информация об аннулированном сертификате ключа проверки электронной подписи Оператора Удостоверяющего центра в список отозванных сертификатов 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 в реестре Удостоверяющего центра. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра информация о сертификате ключа проверки электронной подписи Оператора Удостоверяющего центра в список отозванных сертификатов не заносится.

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

Подача заявления на прекращение действия сертификата ключа проверки электронной подписи осуществляется Оператором Удостоверяющего центра посредством почтовой или курьерской связи по форме Приложения № 8.

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

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

При принятии положительного решения Администратор Удостоверяющего центра прекращает действие сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра.

8.5.2. Прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра по заявлению на отзыв доверенности

Уполномоченная организация вправе отозвать сертификаты ключей проверки электронной подписи своих полномочных представителей – Операторов Удостоверяющего центра, путем подачи заявления на отзыв доверенности Оператора Удостоверяющего центра.

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

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

В случае отказа в прекращении действия сертификатов ключей проверки электронной подписи Удостоверяющий центр уведомляет об этом Уполномоченную организацию.

При принятии положительного решения Администратор Удостоверяющего центра прекращает действие сертификатов ключей проверки электронной подписи Оператора Удостоверяющего центра.

8.6. 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 в бумажной форме;
- по заявлению 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 составляет 15 (Пятнадцать) дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то действие данного сертификата прекращается Удостоверяющем центром.

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

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

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

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

После получения Удостоверяющим центром заявления на приостановление действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего

дня, следующего за рабочим днем, в течение которого заявление было принято Удостоверяющим центром.

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

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

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

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

Заявление подается в Удостоверяющий центр по телефону.

Оператор Удостоверяющего центра должен сообщить Администратору Удостоверяющего центра следующую информацию:

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

Заявление Удостоверяющим центром принимается только в случае положительной аутентификации Оператора Удостоверяющего центра (совпадения ключевой фразы, сообщенной Оператором Удостоверяющего центра по телефону, и ключевой фразы, хранящейся в Удостоверяющем центре).

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

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

При принятии положительного решения, Администратор Удостоверяющего центра приостанавливает действие сертификата ключа проверки электронной подписи.

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

8.6.3. Приостановление действия сертификата ключа проверки электронной подписи 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.

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

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

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра только по его владельца и только в том случае, если действие сертификата ключа проверки электронной подписи было приостановлено.

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

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

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

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

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

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

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

8.8. Подключение Информационной системы Уполномоченной Организации к Сервису электронной подписи

Удостоверяющий центр предоставляет Уполномоченной организации Прикладной интерфейс подключения к Сервису электронной подписи в соответствии с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика». 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.

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

Подключение Стороннего центра идентификации Уполномоченной организации к Сервису электронной подписи осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению от Уполномоченной Организации по форме в соответствии с Приложение № 15. Заявление передается в Удостоверяющий центр курьерской или почтовой связью. Вместе с заявлением на носителе информации передается сертификат, используемый для проверки подписи SAML-токенов, передаваемых от Стороннего центра идентификации.

Настройка параметров СЭП для подключения Стороннего центра идентификации Уполномоченной Организации осуществляется в течение 5 (Пяти) рабочих дней с даты получения подписанного заявления по форме в соответствии с Приложение № 15.

Сторонний центр идентификации подключается на период действия предоставленного сертификата Стороннего центра идентификация.

При смене Уполномоченной организацией сертификата Стороннего центра идентификации осуществляется повторное подключение Стороннего центра идентификации в соответствии с п.8.9 настоящего Регламента.

Заявление на подключение 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, созданных Удостоверяющим центром.

Регистрацию Оператора СЦИ в СЭП выполняет Удостоверяющий центр после получения заявления по форме в соответствии с Приложением № 19. Заявление передается в Удостоверяющий центр курьерской или почтовой связью.

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

8.10. Подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи

Подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению от Уполномоченной Организации по форме в соответствии с Приложение № 16. Заявление передается в Удостоверяющий центр курьерской или почтовой связью.

Заявление на подключение SMS-шлюза может быть отправлено Администратору Удостоверяющего центра в электронной форме, подписанное электронной подписью Оператора УЦ и руководителя Уполномоченной организации с использованием сертификатов, созданных Удостоверяющим центром.

Настройка параметров СЭП для подключения SMS-шлюза Уполномоченной организации осуществляется в течение 5 (Пяти) рабочих дней с даты получения подписанного заявления по форме в соответствии с Приложение № 16.

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.

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

Проверка актуального статуса сертификатов ключей проверки электронной подписи, выданных Уполномоченной организацией, осуществляется с использованием СЭП.

Получение документированной информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется на основании заявления, направляемого Оператором Удостоверяющего центра. Данное заявление оформляется по форме Приложения №12 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

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

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

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

8.12. 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 проведение экспертных работ по подтверждению 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.

В данном случае для подтверждения подлинности ЭП в электронных документах Оператор Удостоверяющего центра подает заявление в Удостоверяющий центр по форме, приведенной в Приложении №13.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность 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).

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

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

Заключение содержит:

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

Отчет по выполненной проверке содержит:

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

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

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет десять рабочих дней с момента поступления заявления в Удостоверяющий центр.

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

8.13. 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 по форме Приложения № 18, 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 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 одноразовым паролем, переданного заявителю от СЭП посредством информационного сообщения или сформированная им с использованием OTP-токена, полученного от Оператора УЦ.

Регистрация всех операций, выполняемых Операторами 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 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, выданных Уполномоченной организацией.

Владелец сертификата ключа проверки электронной подписи Пользователя УЦ подтверждает использование своего ключа электронной подписи посредством ввода индивидуального ПИН-кода доступа к ключу электронной подписи и одноразового пароля, формируемого СЭП и отправляемого в информационном сообщении на номер мобильного телефона владельца сертификата, 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.

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

Удостоверяющий центр предоставляет актуальную информации о статусе сертификатов 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 OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭП Службы актуальных статусов сертификатов в OCSP-ответе;
- Сертификат ключа подписи Службы актуальных статусов сертификатов на момент подтверждения подлинности ЭП OCSP-ответа действителен;
- Ключ электронной подписи Службы актуальных статусов сертификатов на момент формирования OCSP-ответа действителен;
- Сертификат ключа проверки электронной подписи 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 в штампе времени;
- Сертификат ключа проверки электронной подписи Службы штампов времени на момент подтверждения подлинности ЭП штампа времени действителен;
- Ключ электронной подписи Службы штампов времени на момент формирования штампа времени действителен;
- Сертификат ключа проверки электронной подписи 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.

9. Структура сертификатов ключей проверки электронной подписи и сроки действия ключевых документов

9.1. Структура сертификата ключа проверки электронной подписи Удостоверяющего центра

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

9.2. Структура сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийныйномер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритмподписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по (notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество OrganizationUnit = Подразделение Organization = Организация Locality = Город Country = Страна = RU E = Электронная почта Компонента имени CN и O обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата
PublicKey	Открытый ключ	Ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТР 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Электронная подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Оператор DSS - (1.2.643.2.2.34.32) Проверка подлинности клиента - (1.3.6.1.5.5.7.3.2)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа электронной владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора ключа электронной подписи Удостоверяющего центра, с использованием которого создан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP

9.3. Структура сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (клиентский сертификат ключа проверки электронной подписи)

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийныйномер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритмподписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО Organization(Организация) = ООО КРИПТО-ПРО Locality(Город)= Москва Country(Страна)= RU Email(Электронная почта) = cpca@cryptopro.ru
ValidityPeriod	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата и Оператором Удостоверяющего центра. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
PublicKey	Открытый ключ	Ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТР 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Электронная подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Application Policy	Политика применения	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора ключа электронной подписи Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа проверки электронной подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

9.4. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ КРИПТО-ПРО – псевдоним Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (ResonCode) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата ключа проверки электронной подписи (корневого сертификата) Удостоверяющего Центра

9.5. Расширения KeyUsage, ExtendedKeyUsage, ApplicationPolicy сертификата ключа проверки электронной подписи содержат сведения об отношениях, при осуществлении которых электронный документ, подписанный ЭП, будет иметь юридическое значение. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре и определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение приведен в Приложении № 1 настоящего Регламента.

9.6. Сроки действия ключевых документов

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

9.6.2. Срок действия ключа электронной подписи Оператора Удостоверяющего центра составляет 1 (один) год.

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

Срок действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра не превышает 1 (один) год. Время начала периода действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «ValidityPeriod» соответственно.

9.6.3. Срок действия ключа электронной подписи Пользователя Удостоверяющего центра составляет 1 (один) год.

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

Срок действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра не превышает 1 (Один) год. Время начала периода действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «ValidityPeriod» соответственно.

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 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, 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, 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 совпадает со значением поля notAfter поля Validity сертификата ключа проверки электронной подписи Удостоверяющего центра). Изданный список отозванных сертификатов публикуется Удостоверяющим центром, изготовление нового списка отозванных сертификатов, 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, 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, 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, действие которых было приостановлено, подлежат внеплановой смене.

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 Оператор связывается с Удостоверяющим центром по телефону и приостанавливает действие сертификата, соответствующего ключу, конфиденциальность которого нарушена, посредством подачи заявления на приостановление действие сертификата в устной форме (пункт 8.6.2 настоящего Регламента).

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

10.4. Нарушение конфиденциальности ключевых документов Пользователя Удостоверяющего центра

Пользователь 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 Пользователь связывается с Удостоверяющим центром по телефону и приостанавливает действие сертификата, соответствующего ключу, конфиденциальность которого нарушена, посредством подачи заявления на приостановление действие сертификата в устной форме.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр прекращает действие данного сертификата.

10.5. Конфиденциальность информации

10.5.1. Типы конфиденциальной информации

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

10.5.1.2. Персональная и корпоративная информация об Операторах и Пользователях Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

10.5.1.3. 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.

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

10.5.2. Типы информации, не являющейся конфиденциальной

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

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

10.5.2.3. Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, создаваемые Удостоверяющим центром, не считается конфиденциальной.

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

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

10.5.3. Исключительные полномочия Удостоверяющего центра

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

10.6. 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.

10.7. Прекращение оказания услуг Удостоверяющим центром

10.7.1. 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, решение по созданию и выдаче которых принял Оператор Удостоверяющего центра, по усмотрению Удостоверяющего центра может быть прекращено. От Сервиса электронной подписи отключаются все Сторонние центры идентификации и SMS-шлюз Уполномоченной jрганизации.

10.8. Непреодолимая сила (форс-мажор)

10.8.1. 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

10.8.2. 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.

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

10.8.4. 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

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

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

11. Список приложений

11.1. Приложение № 1. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «КРИПТО-ПРО», определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение

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

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

11.4. Приложение № 4. Форма доверенности на предоставление заявительных документов, получение ключа электронной подписи и сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

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

11.6. Приложение № 6. Форма заявления на создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (при генерации ключей подписи на рабочем месте Оператора с использованием файла запроса)

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

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

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

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

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

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

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

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

11.15. Приложение № 15. Форма заявления на подключение к Сервису электронной подписи Стороннего центра идентификации Уполномоченной организации

11.16. Приложение № 16. Форма заявления на подключение к Сервису электронной подписи SMS-шлюза Уполномоченной организации

11.17. Приложение № 17. Функции Сервиса электронной подписи

11.18. Приложение № 18. Перечень параметров функционирования Сервиса электронной подписи для настройки доступа Операторов и Пользователей УЦ

11.19. Приложение № 19. Форма заявления на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации.

Приложение №1 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Список объектных идентификаторов (OID), зарегистрированных в
Удостоверяющем центре ООО «КРИПТО-ПРО»)

Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «КРИПТО-ПРО», определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение

	OID	Область применения
1.	1.2.643.2.2.34.32	Оператор DSS – аутентификация Оператора Удостоверяющего центра при подключении к Сервису электронной подписи и подписания электронных документов, определенных Регламентом
2.	1.3.6.1.5.5.7.3.9	Подпись ответа службы OCSP – формирование электронной подписи ответов Службы актуальных статусов сертификатов
3.	1.3.6.1.5.5.7.3.8	Установка штампа времени – формирование электронной подписи штампов времени, предоставляемых Службой штампов времени

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит зарегистрировать уполномоченного представителя

_____
(фамилия, имя, отчество)

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

Настоящим _____
(фамилия, имя, отчество)

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

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)

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

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

«___»_____20__ г.

М.П.

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

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

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

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

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

подтверждаю.

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

«___»_____20__ г.

М.П.

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

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

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

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

2. Получить необходимые лицензии на право пользования программного обеспечения для Оператора Удостоверяющего центра ООО «КРИПТО-ПРО», сертификат ключа проверки электронной подписи (корневого сертификата) Удостоверяющего центра ООО «КРИПТО-ПРО» и иные документы, определенные Регламентом Удостоверяющего центра ООО «КРИПТО-ПРО»

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

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

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

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

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

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

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

«___»_____20__ г.

М.П.

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

Заявление на создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

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

CommonName (CN)[1]	Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
OrganizationUnit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Contry (C)	RU	
ExtendedKeyUsage	Проверка подлинности клиента Оператор DSS	(1.3.6.1.5.5.7.3.2) (1.2.643.2.2.34.32)

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

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

«___»_____20__ г.

М.П.

[1] - Обязательными для заполнения полями (расширениями) являются CommonName (CN) и ExtendedKeyUsage. Необходимость установления значений остальных полей определяется заявителем

Приложение №6 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на создание сертификата на основе файла запроса при генерации ключей на рабочем месте Оператора Удостоверяющего центра)

Заявление на создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

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

CommonName (CN)[1]	Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
OrganizationUnit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Contry (C)	RU	
ExtendedKeyUsage	Проверка подлинности клиента Оператор DSS	(1.3.6.1.5.5.7.3.2) (1.2.643.2.2.34.32)

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

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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC4jCCAo8CAQAwgYAxITAfBgkqhkiG9w0BCQEWEml2YW5vdkBtLXJlZXN0ci5y
dTELMAkGA1UEBhMCUlUxDzANBgNVBAcTBk1vc2NvdzEVMBMGA1UEChMMT3JnYW5p
emF0aW9uMQ0wCwYDVQQLEwREZXB0MRcwFQYDVQQDEw5JdmFuIEkuIEl2YW5vdjBj
MBwGBiqFAwICEzASBgcqhQMCAiQABgcqhQMCAh4BA0MABEBog51WRaScCe7qMJ3g
2s+zrO8y4G5VhcaIdxWIYKWmcHL8AHKGC2pmOWCmE/XzUZorhycAYrUaH0gstA9C
```

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

nz17oIIBoDAaBgorBgEEAYI3DQIDMQwWCjUuMC4yMTk1LjIwYwYKKwYBBAGCNwIB
DjFVMFMwDgYDVR0PAQH/BAQDAgTwMBkGCSqGSIb3DQEJDwQMMAowCAYGKoUDAgIV
MCYGA1UdJQQfMB0GCCsGAQUFBwMCBggrBgEFBQcDBAYHKoUDAgIiBjCCARsGCisG
AQQBgjcNAgIxggELMIIBBwIBAR52AEMAcgB5AHAAdABvAC0AUAByAG8AIABHAE8A
UwBUACAAUgAgADMANAAuADEAMAAtADIAMAAwADEAIABDAHIAeQBwAHQAbwBnAHIA
YQBwAGgAaQBjACAAUwBlAHIAdgBpAGMAZQAgAFAAcgBvAHYAaQBkAGUAcgOBiQAk
ofCLPzGSbmXMEex/cq9WymQT+3kQlCRX0bRnOsMlGVV4AxJLfMS5x1PX/wWKxIv9
vnjdFdnXcklLJ5cw8g9kkpMzdNEcEMgPYEi0xttZ9r3aTsIEjBEn7+1h8IgY+yDy
deR9DgPvC/QFS0diXCWYESkt2PiiAyAY/4WmVS1NSwAAAAAAAAAMAoGBiqFAwIC
AwUAA0EAixD6RSeDYbF/VVjPfi+H+klhKaz5MbFNRa9BVIViFS3ccRvNZVpEfUFx
HriROkQQa3/9hfEWRAupRwMye/3CMg==
-----ENDNEWCERTIFICATEREQUEST-----

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

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

«___»_____20__ г.

М.П.

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

Заявление на создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

Сведения о запросе на сертификат:
Этот запрос:
Кем выпущен:
User1
Версия: 1 (0x0)
Субъект запроса на сертификат: CN = User1
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9
Атрибуты запроса на сертификат X.509
1. Атрибут 1.3.6.1.4.1.311.13.2.3
Название: Версия ОС
Значение: 5.0.2195.2
2. Атрибут 1.3.6.1.4.1.311.2.1.14
Название: Расширения сертификатов
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 1.2.840.113549.1.9.15
Название: Возможности SMIME
Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
3. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Оператор DSS (1.2.643.2.2.34.32) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
Атрибут 1.3.6.1.4.1.311.13.2.2
Название: CSP заявки
Сведения о провайдере
Назначение ключа: ОБМЕН
Название провайдера:Crypto-Pro GOSTR 34.10-2001CryptographicServiceProvider
Подпись провайдера: AA03 C083 A1B5 CCDC 20A0 F6A9 29D0 F124 8374 2251 6F71 C51A 52D5 469B 684B 7B7D 342F E0D8 8DDB 09EB B3BF 8DA6 3C98 AF07 327E 7EEB A121 A372 CA57 030A 87D2 AFA9 CDBB D3AA 7575 AA85 01B7 0AB3 79B5 98BA 8453 9B62 AA33 AA4C F07E 6043 64AB BCA5 0A4B EB59 A3D0 E55B D306 78A8 0B0B B05E 79F0 9001 E7B1 E133 B708 C11D 6AA1 4423 0000 0000 0000 0000
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТР 34.11/34.10-2001
Параметры: 0500
Значение: BABC 1455 ADA3 DC7F 0EC9 3A1A 5020 C0DE F561 C757 2986 BB2E B180 A5B0 091A 7F0A 6FA1 1A6E EE48 A366 B904 7288 A311 D966 BB2F FC7C EB75 3F0A 49ED A651 3E10 258A

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

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

«___»_____20__ г.

М.П.

Приложение №8 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на прекращение действия (аннулирование) сертификата)

Заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

в связи с _____
(причина отзыва сертификата)

Просит прекратить действие сертификата ключа проверки электронной подписи своего уполномоченного представителя – Оператора Удостоверяющего Центра ООО «КРИПТО-ПРО»: _____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

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

Подпись владельца сертификата ключа проверки электронной подписи – Оператора Удостверяющего центра ООО «КРИПТО-ПРО» _____ /_____/

«____» _____ 20____ г.

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

«___»_____20__ г.

М.П.

Приложение №9 к Регламенту Удостоверяющего Центра
ООО «КРИПТО-ПРО»
(Форма заявления на отзыв доверенности)

Заявление на отзыв доверенности

_____
(наименование организации, включая организационно-правовую форму)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

и просит прекратить действие сертификатов ключей проверки электронной подписи, содержащие область использования - Оператор Центра Регистрации (1.2.643.2.2.34.5), владельцем которых является данный Оператор Удостоверяющего центра ООО «КРИПТО-ПРО».

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

«___»_____20__ г.

М.П.

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

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

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

Подпись владельца сертификата ключа проверки электронной подписи – Оператора Удостверяющего центра ООО «КРИПТО-ПРО» _____ /_____/

«____» _____ 20____ г.

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

«___»_____20__ г.

М.П.

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

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

Подпись владельца сертификата ключа проверки электронной подписи – Оператора Удостверяющего центра ООО «КРИПТО-ПРО» _____ /_____/

«____» _____ 20____ г.

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

«___»_____20__ г.

М.П.

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

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

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

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

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

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

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

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

«____» _____ 20____ г.

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

Приложение №13 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на подтверждение подлинности ЭП)

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 ЭЦП формата CMS, на прилагаемом к заявлению носителе – рег. № МД–XXX

3. Время[4] 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.

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

Приложение №14 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма печати копии сертификата ключа проверки электронной подписи)

Копия сертификата ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан:
Фамилия Имя Отчество
Кем выдан:
CryptoProCA
Действителен с 15 октября 2003 г. 12:03:00 UTC по 15 октября 2004 г. 12:12:00 UTC
Версия: 3 (0x2)
Серийный номер: 14F5 9CF2 0000 0000 003A
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Издатель сертификата: CN = CryptoPro CA, C = RU
Срок действия:
Действителен с: 15 октября 2003 г. 12:03:00 UTC
Действителен по: 15 октября 2004 г. 12:12:00 UTC
Владелец сертификата: CN = User1
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-94
Идентификатор: 1.2.643.2.2.20
Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Оператор DSS (1.2.643.2.2.34.32) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 56BD CA83 3029 0673 CA83 3381 16D4 AF10 C3D6 9A75
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=50AA 3E1E 4186 F8DC 3585 6E11 2C11 D9E3 0A91 7AD7 Поставщик сертификата: Адрес каталога: CN=CryptoPro CA C=RU Серийный номер сертификата=29D1 B0C8 C311 ACAE 48DB AAB1 3687 CEFC
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Значение: 826C DDFB 331C 58C5 FD3D 9233 4A1D 2D7A B973 387C 8E8A DD3D 6FCE 0573 508A 3DC4 B29F 5961 FB6C D1EB 1B40 37C7 8473 5B0F FECA 5E38 EA0C 3890 C77A C97E BD18 873A

Подпись уполномоченного лица УЦ: _____/_____

«____» _____ 20__ г.

Печать Удостоверяющего Центра

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

Приложение №15 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на подключение Стороннего центра идентификации)

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

_____
(полное наименование 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. 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, 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 №16 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на подключение SMS-шлюза)

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

_____
(полное наименование 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:

№ п/п	Параметр СЭП	Настраиваемое значение параметра СЭП
1.	URL и сетевой (IP) адрес SMS-шлюза	URL-адрес SMS-шлюза Уполномоченной организации
		Сетевой (IP) адрес и номер порта SMS-шлюза Уполномоченной организации
2.	Идентификационные данные	Логин и пароль для подключения к SMS-шлюзу Уполномоченной организации
3.	ФИО	Работник Уполномоченной Организации, ответственный за подключение и функционирование SMS-шлюза Уполномоченной организации, и его контактные данные:
4.	Подразделение	Ответственного работника Уполномоченной Организации
5.	Рабочий адрес электронной почты	Ответственного работника Уполномоченной Организации
6.	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 №17 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(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 34.10-2001 «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. Электронная подпись ГОСТ 34.10 – 2001;
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 с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика».

Аутентификация пользователей осуществляется по протоколу SAML 2.0 (WS Security) с использованием Стороннего центра идентификации Уполномоченной организации, подключаемого к Сервису электронной подписи в соответствии с документом

«ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора».

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

Вторичная аутентификация пользователей осуществляется посредством одноразового кода, высылаемого Пользователям Удостоверяющего центра 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 должен 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 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 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 (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 (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.

Приложение №18 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(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 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:

№ п/п	Параметр СЭП	Настраиваемое значение параметра СЭП	
1.	URL-адрес веб-интерфейса СЭП для подключения Пользователей УЦ	Вида https://www.justsign.me/<company-name> или «Не предоставлять».	
		Порт доступа и алгоритм шифрования трафика (TLS)	*Например: 443 (RSA), 80*
2.	URL-адрес прикладного интерфейса СЭП	Вида https://www.justsign.me/< company-name>ss	
		Порт доступа и алгоритм шифрования трафика (TLS)	*Например: 443 (RSA), 80*
3.	URL-адрес Центра идентификации СЭП	Вида https://www.justsign.me/<company-name>idp	
		Порт доступа	443, 80
4.	URL-адрес веб-интерфейса СЭП для подключения Оператора	Вида https://www.justsign.me/<company-name>idp/admins/	
		Порт доступа и алгоритм шифрования трафика (TLS)	4430, 4431, 4432 (ГОСТ)
5.	URL-адрес сервиса проверки ЭП	https://www.justsign.me/verifycpca	
		Порт доступа	443
6.	Сетевые адреса (IP) СЭП (Определяет УЦ)	193.37.157.2 193.37.157.3	
7.	Сетевые адреса (IP) источника (SOAP-запросов при подключении ИС)	Определяет УО при подключении к СЭП (*вида 777.77.7.77*)	
8.	Уникальный идентификатор Центра идентификации СЭП	Определяет УЦ при подключении УО	
9.	Отпечаток сертификата (значение хэш sha1) Центра идентификации СЭП	Определяет УЦ при подключении УО	
10.	Отображаемое наименование группы пользователей (1).	Опционально. Если не указан – используется группа по умолчанию для всех пользователей. Указать для всех планируемых групп в дополнительных пунктах.	
		Уникальный идентификатор группы пользователей (1).	Определяет УЦ для каждой указанной УО группы.
11.	Форматы подписи, доступные в Web-	Оставить требуемые из перечня:	

	интерфейсе пользователя	1. «Чистая» ЭП ГОСТ 34.10 – 2001; 2. CAdES-BES/ X Long Type 1; 3. XMLDSig; 4. PDF-CMS/CAdES; 5. MS Office.
12.	Саморегистрация Пользователей УЦ	Разрешена/запрещена (по умолчанию Разрешена)
13.	Режим создания учетных записей в СЭП для пользователей сторонних ЦИ	Автоматический при первом подключении/ Оператором (по умолчанию – Автоматический)
14.	Возможность блокирования пользователей Оператором	Разрешено/Запрещено (по умолчанию Разрешено)
15.	Автоматическое создание сертификатов по запросу Пользователей УЦ	Разрешена/Запрещена (по умолчанию Запрещено)
16.	Автоматическое управление и обновление сертификатов по запросу Пользователей УЦ (при наличии действующего сертификата Пользователей УЦ)	Разрешено/Запрещено (по умолчанию Запрещено)
17.	Вторичная аутентификация пользователей	Обязательна/Не обязательна/Управляется по пользователям (по умолчанию Управляется по пользователям)
18.	Вторичная аутентификация по умолчанию (указывается при выборе для п.17 значения «Управляется по пользователям»)	Обязательна/Не обязательна (по умолчанию Обязательна)
19.	Возможность изменения пользователем параметров вторичной аутентификации (указывается при выборе для п.17 значения «Управляется по пользователям»)	Разрешено/Запрещено (по умолчанию Запрещено)
20.	Подтверждение телефона (с отправкой СМС)	Требуется/Не требуется (по умолчанию Требуется)
21.	Максимальное время жизни маркера (в секундах)	От 1 до 2147483647 (по умолчанию 1800)
22.	Время жизни маркера по умолчанию (в секундах), если не задано в запросе на подключение	От 1 до 2147483647 (по умолчанию 600)
23.	Время действия подтверждённой операции (в секундах)	От 1 до 2147483647 (по умолчанию 300)
24.	Длина долговременных паролей (в символах)	От 1 до 256 (по умолчанию 8)
25.	Сложность долговременных паролей	1 – только цифры 2 – цифры и буквы, 3 – цифры и буквы в разном регистре, 4 – цифры, буквы в разном регистре и спец символы (по умолчанию 3)
26.	Максимальное количество попыток ввода долговременного пароля до блокирования учетной записи	От 0 до 2147483647, 0 – блокирование отключено (по умолчанию – 5)
27.	Длина одноразовых паролей	От 1 до 256 (по умолчанию – 5)
28.	Сложность одноразовых паролей	1 – только цифры 2 – цифры и буквы, 3 – цифры и буквы в разном регистре, 4 – цифры, буквы в разном регистре и спец символы (по умолчанию – 1)
29.	Максимальное количество попыток ввода	От 0 до 2147483647, 0 – блокирование

	одноразового пароля	отключено (по умолчанию – 3)
30.	Время действия одноразового пароля (в секундах)	От 1 до 2147483647 (по умолчанию 300)
31.	Минимальное время жизни одноразового пароля (в секундах) – до возможности запроса нового пароля, пока не введен старый.	От 1 до 2147483647 (по умолчанию 300)
32.	Максимальный размер поля с информацией о документе, попадающей в SMS (в символах)	От 0 до 256 (по умолчанию 256)
33.	Использование ПИН-кода для ключевого контейнера	Требовать/ Не требовать/Позволять задавать (по умолчанию - Позволять задавать)
34.	Перечень событий для рассылки уведомлений Пользователям и Операторам СЭП	В соответствии с Руководством Администратора ПАК «КриптоПро DSS» п. 9.1, Таблица 87, 88.
35.	Перечень адресов электронной почты и номеров мобильных телефонов для рассылки уведомлений Операторам о событиях СЭП	С условием получения разрешения от владельцев адресов и мобильных телефонов
36.	Дополнительные условия (кастомизация Web-интерфейса пользователя/оператора, иконка стороннего ЦИ, набор компонент имени отображаемых пользователю/оператору в Web -интерфейсе ЦИ, регистрация специальных OID и шаблонов сертификатов и т.п.)	Указывает УО

_____ _____ /_____/

«____» _____ 20____ г.

_____ _____ /_____/

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

«___»_____20__ г.

М.П.

Приложение №19 к Регламенту Удостоверяющего центра
ООО «КРИПТО-ПРО»
(Форма заявления на регистрацию Оператора Стороннего
центра идентификации)

Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации

_____
(полное наименование 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

Настоящим _____
(фамилия, имя, отчество полномочного представителя)
_____
(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных ООО «КРИПТО-ПРО».

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)

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

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

М.П.