Утвержден
Приказом ООО «КРИПТО-ПРО»
от «01» декабря 2017 г. № 7

РЕГЛАМЕНТ
ООО «КРИПТО-ПРО»
по предоставлению услуг Сервиса электронной подписи
(Схема обслуживания: распределенная с оператором)

Редакция № 1

г. Москва
2017

1. Сведения об Исполнителе услуг

Общество с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО», именуемое в дельнейшем «Исполнитель», зарегистрировано на территории Российской Федерации в городе Москва (Свидетельство о внесении записи в единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 01 июля 2002 года серия 77 №007360250 от 23.01.2003 г.).

Исполнитель оказывает комплекс услуг, связанных с предоставлением доступа к Сервису электронной подписи, на основании лицензий, опубликованных в сети Интернет по адресу: https://www.cryptopro.ru/about/licenses.

Реквизиты Исполнителя:

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

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

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

ИНН/КПП: 7717107991/771901001

ОГРН: 1037700085444

Код по ОКВЭД2: 62.01, 62.02, 62.03, 62.09, 63.11, 71.20, 74.90, 26.20, 58.29, 46.51, 46.66, 72.19

Код по ОКПО: 51282566

Контактные телефоны, факс, адрес электронной почты:

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

2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Договором на предоставление услуг сервиса электронной подписи (далее - Договор), настоящим Регламентом и Федеральным законом «Об электронной подписи», а именно:

Администратор Сервиса электронной подписи (Администратор СЭП) – ответственный работник Исполнителя, обеспечивающий регистрацию Операторов СЭП и бесперебойное функционирование СЭП в соответствии с настоящим Регламентом.

Веб-интерфейс Сервиса электронной подписи (Веб-интерфейс СЭП) – интерфейс взаимодействия Пользователя *СЭП* и Оператора *СЭП* с 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-сервере *СЭП*.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в соответствии с законодательством Российской Федерации создан сертификат ключа проверки электронной подписи посредством СЭП.

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, созданная посредством СЭП и предназначенная для создания электронной подписи.

Ключ электронной подписи СЭП – ключ электронной подписи, использующийся в СЭП для подписания запросов на создание сертификатов и управления ими, а также защищенного подключения к Удостоверяющему центру при наличии доступа.

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

Многофакторная аутентификация - процедура проверки подлинности Пользователя СЭП при осуществлении доступа с использованием двух и более уникальных характеристик, известных или присущих только Пользователю СЭП (факторов аутентификации). При управлении доступом к Сервису электронной подписи для первичной аутентификации Пользователя СЭП используется постоянно действующий пароль, самостоятельно определяемый Пользователем СЭП, для вторичной аутентификации может использоваться код аутентификации HMAC с помощью ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS» или одноразовый пароль, формируемый Сервисом электронной подписи и высылаемый Пользователю СЭП в информационном сообщении на номер мобильного телефона, указанный Пользователем СЭП при регистрации, или OTP-токеном, выдаваемым Оператором СЭП по заявлению Пользователя СЭП. Уполномоченная организация вправе использовать дополнительные факторы аутентификации для управления доступом Пользователей СЭП к Сервису электронной подписи совместно с собственным Сторонним центром идентификации.

Оператор Стороннего центра идентификации (Оператор СЦИ) – Оператор СЭП, зарегистрированный в Стороннем центре идентификации Уполномоченной организации, действующий от имени Уполномоченной организации по обеспечению создания ключей электронной подписи и запросов на создание управление сертификатами ключей проверки электронной подписи Пользователей СЭП, зарегистрированных в том же Стороннем центре идентификации Уполномоченной организации.

Оператор Сервиса электронной подписи (Оператор СЭП) — физическое лицо, действующее от имени Уполномоченной Организации, совершающее действия по регистрации пользователей в Сервисе электронной подписи и управлению параметрами доступа пользователей к Сервису электронной подписи, а также по обеспечению создания ключей электронной подписи, запросов на создание и управление сертификатами ключей проверки электронной подписи Пользователей СЭП.

Пользователь - физическое лицо, намеревающееся стать Пользователем Сервиса электронной подписи.

Пользователь Сервиса электронной подписи (Пользователь СЭП) –физическое лицо, зарегистрированное в СЭП или в Стороннем центре идентификации и являющееся владельцем ключа электронной подписи, созданного посредством СЭП, либо физическое лицо, действующее от имени владельца ключа электронной подписи, созданного посредством СЭП, если владелец ключа электронной подписи – юридическое лицо, и указанное в соответствующем 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 СЭП (API) – интерфейс подключения Информационных систем Уполномоченной организации к СЭП с использованием сети передачи данных для получения доступа к функциям электронной подписи, формирования запросов на создание и управление сертификатами ключей проверки электронной подписи, реализованный 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 СЭП.

ПО – программа для ЭВМ ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS».

Правообладатель - обладатель исключительных прав на ПО. Правообладателем ПО является ООО «КРИПТО-ПРО.

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

Регламент Сервиса электронной подписи (Регламент) – настоящий документ, определяющий порядок предоставления услуг Сервиса электронной подписи.

Регистрационные данные Пользователя СЭП - идентификационная информация, содержащая сведения о Пользователе СЭП, имеющему право доступа к СЭП, и используемая при создании Сертификата Пользователя СЭП (содержится в сведениях о владельце этого сертификата (в расширении Subject Name)).

Сервис электронной подписи (СЭП) - комплекс организационных, технических и программных средств Исполнителя, обеспечивающих для Пользователей СЭП удаленную реализацию функций централизованного создания и хранения ключей электронной подписи, создания и проверки усиленной 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 к СЭП осуществляется посредством Веб-интерфейса, предоставляемого Исполнителем, или подключенной к СЭП Информационной системы Уполномоченной организации.

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

Сертификат ключа проверки электронной подписи Оператора СЭП *(Сертификат Оператора* СЭП*)* - сертификат ключа проверки электронной подписи, используемый для аутентификации Оператора СЭП при подключении к СЭП, получаемый в Удостоверяющем центре.

Сертификат ключа проверки электронной подписи Сервиса электронной подписи (Сертификат СЭП) – сертификат ключа проверки электронной подписи, принадлежащий Исполнителю и используемый для проверки электронной подписи, запросов на создание сертификатов ключа проверки электронной подписи и управления ими, а также аутентификации СЭП при подключении к Удостоверяющему центру при наличии доступа.

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 ключа проверки электронной подписи, созданных Удостоверяющим центром.

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

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

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

Список отозванных сертификатов (СОС) – электронный документ с 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 ЭП) – 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 (СЦИ) – система аутентификации 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 управления доступом Пользователей СЭП к СЭП.

Удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей Пользователей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».

Уполномоченная организация – юридическое лицо, заключившее с Исполнителем Договор.

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 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)».

HMAC – криптографическая функция HMAC_GOSTR3411_2012_256, описанная в документе «Технический комитет 26. Рекомендации по стандартизации. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012» для формирования и использования кода аутентификации с помощью специальной программы для ЭВМ ПО «Модуль аутентификации myDSS для ПАК «КриптоПро DSS»;

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 при осуществлении доступа к СЭП и подтверждения использования принадлежащего Пользователю СЭП ключа электронной подписи.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. СЭП функционирует в соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на создание 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 СЭП одноразовых паролей и уведомлений о выполняемых операциях (транзакциях).

3. Общие положения

3.1. Предмет Регламента

3.1.1. Настоящий Регламент разработан в соответствии с положениями Договора и действующим законодательством Российской Федерации, регулирующим деятельность, связанную с использованием электронной подписи.

3.1.2. Сторонами Регламента являются Исполнитель и Уполномоченная организация.

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

3.2. Применение Регламента

3.2.1. 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.

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

3.2.3. В случае противоречия и (или) расхождения положений Регламента с положениями Договора, Стороны считают доминирующим смысл и формулировки Договора.

3.3. Изменение Регламента

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

3.3.2. Уведомление о внесении изменений в Регламент осуществляется Исполнителем путем обязательного размещения указанных изменений на сайте Исполнителя по адресу: http://dss.cryptopro.ru/reglament/reglamentoperdss.pdf.

3.3.3. Все изменения, вносимые Исполнителем в Регламент, вступают в силу и становятся обязательными по истечении 20 (двадцати) рабочих дней с даты размещения указанных изменений и дополнений на сайте Исполнителя, за исключением изменений, вносимых в связи с изменением действующего законодательства Российской Федерации, которые вступают в силу одновременно с вступлением в силу соответствующих нормативных правовых актов, повлекших изменение законодательства Российской Федерации.

3.3.4. Любые изменения, вносимые в Регламент с момента их вступления в силу, распространяются равно на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений в силу.

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

4. Предоставление информации

4.1. Исполнитель предоставляет Уполномоченной организации 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 Исполнителю.

4.2. Исполнитель 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 позднее чем за один месяц до момента запроса Исполнителю;
- 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 СЭП (либо нотариально заверенные копии этих документов);
- иные документы, установленные Регламентом и Договором, а также дополнительные документы по усмотрению Исполнителя.

5. Права и обязанности сторон

5.1. Исполнитель обязан:

5.1.1. Использовать в составе СЭП для создания и хранения ключей электронной подписи, формирования и проверки электронной подписи только сертифицированные в соответствии с требованиями законодательства Российской Федерации средства электронной подписи.

5.1.2. Обеспечить защиту созданных в СЭП ключей электронной подписи от несанкционированного доступа.

5.1.3. По запросу Уполномоченной организации сформировать и предоставить запрос на создание Сертификата СЭП в формате PKCS#10 в соответствии с порядком, установленным Исполнителем.

5.1.4. Установить в СЭП полученный от Удостоверяющего центра Сертификат СЭП.

5.1.5. Использовать ключ электронной подписи СЭП только для подписания формируемых в СЭП запросов на создание Сертификатов Пользователей СЭП и управления ими, а также подключения к СЭП для передачи сформированных запросов и получения созданных Сертификатов СЭП.

5.1.6. Организовать свою работу по московскому времени. Исполнитель обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

5.1.7. Обеспечить уникальность идентификационных данных Операторов СЭП и Пользователей СЭП.

5.1.8. Предоставить аутентифицированным Пользователям СЭП и Операторам СЭП доступ к СЭП и обеспечить круглосуточное функционирование СЭП в режиме 24х7 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 СЭП и Операторам СЭП функциональные возможности СЭП приведены в Приложении № 5 к Регламенту.

5.1.9. Обеспечить уникальность значений создаваемых в СЭП ключей проверки электронной подписи Пользователей СЭП.

5.1.10. Подключить Оператора СЭП для предоставления доступа к СЭП в соответствии с п.8.1 настоящего Регламента.

5.1.11. Прекратить, приостановить и возобновить доступ Оператора СЭП к СЭП в случае прекращения, приостановления и возобновления действия сертификата этого Оператора СЭП, а также по заявлению в соответствии с п.8.3. Регламента.

5.1.12. Предоставить по запросу Уполномоченной организации на уточнение и согласование перечень параметров настройки функционирования СЭП, аутентификации Операторов СЭП и Пользователей СЭП к СЭП по форме в соответствии с Приложением № 6 к Регламенту.

5.1.13. Подключить к СЭП SMS-шлюз Уполномоченной организация в соответствии с п. 8.5 настоящего Регламента.

5.1.14. Подключить к СЭП Стороннего центра идентификации и зарегистрировать Оператора СЦИ в соответствии с п. 8.6 настоящего Регламента.

5.1.15. Подключить к СЭП Удостоверяющий центр в соответствии с п. 8.7 настоящего Регламента.

5.1.16. Предоставить Уполномоченной организации необходимые права для:

5.1.16.1. подключения к СЭП Информационных систем с использованием Прикладного интерфейса СЭП;

5.1.16.2. регистрации Пользователей в СЭП;

5.1.16.3. управления доступом Пользователей СЭП к СЭП, в том числе с использованием Многофакторной аутентификации;

5.1.16.4. управления доступом к СЭП Пользователей СЭП и Операторов СЦИ с использованием подключенного СЦИ;

5.1.16.5. формирования и получения запросов в электронной форме на создание и управление Сертификатами Пользователей СЭП, отправки сформированных запросов в подключенный УЦ;

5.1.16.6. управления уведомлениями Пользователей СЭП посредством электронной почты и информационных сообщений с использованием подключенного SMS-шлюза;

5.1.17. Уведомить Оператора СЭП и Пользователя СЭП в случае получения информации о нарушении конфиденциальности ключа электронной подписи Оператора СЭП и (или) Пользователя СЭП.

5.1.18. Зарегистрировать в СЭП и обеспечить конфиденциальность информации, содержащейся в полученном от Уполномоченной организации файле инициализации OTP-токенов, используемых для многофакторной аутентификации Пользователей СЭП.

5.1.19. По заявлению Уполномоченной организации в соответствии с формой, приведенной в Приложении № 11 к Регламенту, предоставить сведения, а также принять участие в работе разрешительной комиссии для разбора конфликтной ситуации, связанной с применением электронной подписи, созданной с использованием СЭП.

5.1.20. Не позднее, чем за 30 (тридцать) рабочих дней информировать Уполномоченную организацию о проведении обновления Прикладного интерфейса СЭП, предоставить доступ к тестовой версии СЭП с обновленным Прикладным интерфейсом СЭП. Информирование осуществляется путем отправки электронного сообщения на адрес электронной почты, указанный в зарегистрированном Сертификате Оператора СЭП.

5.2. Уполномоченная организация обязана:

5.2.1. С целью обеспечения гарантированного ознакомления Уполномоченной организации с возможными изменениями и дополнениями Регламента не реже одного раза в месяц посещать сайт Исполнителя.

5.2.2. Известить Исполнителя об изменении реквизитов Уполномоченной организации и по требованию Исполнителя предоставить соответствующие подтверждающие документы в течение 5 (пяти) рабочих дней с момента регистрации изменений.

5.2.3. Предоставить Исполнителю Сертификат Оператора СЭП с Заявлением на подключение Оператора СЭП в соответствии с п.8.1. Регламента. Использование предоставленного для получения доступа к СЭП Сертификата СЭП должно соответствовать ограничениям, содержащимся в предоставленном Сертификате СЭП, если такие ограничения были установлены.

5.2.4. Предоставить Исполнителю Сертификат Удостоверяющего центра, используемый при создании Сертификатов Пользователей СЭП и Операторов СЭП.

5.2.5. Обеспечить получение Исполнителем Сертификата СЭП в случае необходимости подключения к Удостоверяющему центру либо использование для подключения к УЦ имеющегося Сертификата СЭП.

5.2.6. Обеспечить защиту подключения своих Информационных систем к СЭП с использованием СКЗИ, совместимых с СКЗИ, используемых в СЭП.

5.2.7. После проведения проверки с использованием тестовых сертификатов согласовать и подписать предоставленный Исполнителем уточненный перечень параметров настройки функционирования СЭП, аутентификации Операторов СЭП и Пользователей СЭП для доступа к СЭП по форме в соответствии с Приложением № 6 к Регламенту. Использование в СЭП юридически-значимых сертификатов ключей проверки электронной подписи до

предоставления Исполнителю подписанного перечня параметров настройки функционирования СЭП запрещается.

5.2.8. Обеспечить многофакторную аутентификацию Пользователей СЭП при управлении доступом к СЭП, в том числе при использовании Стороннего центра идентификации.

5.2.9. Обеспечить конфиденциальность аутентификационных данных Пользователей СЭП и информации, передаваемой в информационных сообщениях посредством SMS-шлюза.

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

5.2.11. Самостоятельно и за свой счет в обязательном порядке предварительно получать от Пользователей СЭП письменное согласие на получение информационных сообщений на номера мобильных телефонов Пользователей СЭП с одноразовыми паролями и уведомлениями о выполняемых СЭП операциях с использованием принадлежащих Пользователям СЭП ключей электронной подписи в соответствии с настоящим Регламентом.

5.2.12. В случае отправки информационных сообщений Пользователям СЭП непосредственно от Исполнителя по письменному запросу предоставить Исполнителю письменное согласие Пользователя СЭП на получение информационных сообщений на номер мобильного телефона Пользователя СЭП в сроки, установленные в запросе Исполнителя.

5.2.13. Оператор СЭП, являющийся уполномоченным представителем Уполномоченной организации, обязан:

5.2.13.1. Для подключения к СЭП использовать совместимые технические и программные средства, соответствующие предъявляемым требованиям безопасности информации.

5.2.13.2. Обеспечить конфиденциальность своих ключей электронной подписи, соответствующих Сертификату Оператора СЭП.

5.2.13.3. Применять для формирования электронной подписи и подключения к СЭП только действующий ключ электронной подписи.

5.2.13.4. Не применять ключ электронной подписи для подключения к СЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

5.2.13.5. Применять ключ электронной подписи для доступа к СЭП 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.

5.2.13.6. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия Сертификата Оператора СЭП, а также к Исполнителю на прекращение или приостановление доступа к СЭП в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности соответствующего ключа электронной подписи.

5.2.13.7. Не использовать для подключения к СЭП ключ электронной подписи, связанный с Сертификатом Оператора СЭП, 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.

5.2.13.8. Не использовать для подключения к СЭП ключ электронной подписи, связанный с Сертификатом Оператора СЭП, 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.

5.2.13.9. Не использовать для подключения к СЭП ключ электронной подписи, связанный с Сертификатом Оператора СЭП, действие которого прекращено или приостановлено.

5.2.13.10. Использовать для создания ключа электронной подписи, соответствующего Сертификату Оператора СЭП средства электронной подписи, совместимые со средствами СЭП и сертифицированные в соответствии с правилами сертификации Российской Федерации.

5.3. Исполнитель имеет право:

5.3.1. Отказать в подключении Оператора СЭП к СЭП в случае ненадлежащего оформления заявления на подключение Оператора СЭП и (или) несоответствия предоставленного Сертификата Оператора СЭП.

5.3.2. Отказать в подключении Оператора СЭП к СЭП в случае не предоставления и/или ненадлежащего предоставления документов, установленных п. 4.2 настоящего Регламента.

5.3.3. Отказать в прекращении, приостановлении и возобновлении доступа Оператора СЭП к СЭП в случае ненадлежащего оформления соответствующего заявления на прекращение, приостановление и возобновление доступа Оператора СЭП к СЭП.

5.3.4. Отказать в прекращении, приостановлении и возобновлении доступа Оператора СЭП к СЭП в случае, если истек установленный срок действия ключа электронной подписи, соответствующего Сертификату Оператора СЭП.

5.3.5. В одностороннем порядке приостановить доступ Оператора СЭП к СЭП с обязательным уведомлением Оператора СЭП об этом и указанием обоснованных причин.

5.3.6. Отказать в предоставлении доступа Пользователей СЭП к СЭП до получения от Уполномоченной Организации подписанного перечня параметров настройки функционирования СЭП по форме в соответствии с Приложением № 6 к Регламенту.

5.3.7. Отказать в подключении Стороннего центра идентификации Уполномоченной организации в случае ненадлежащего оформления заявления на подключение Стороннего центра идентификации в соответствии с Приложением № 8 к Регламенту.

5.3.8. Отказать в подключении SMS-шлюза Уполномоченной организации в случае ненадлежащего оформления заявления на подключение SMS-шлюза в соответствии с Приложением № 7 к Регламенту.

5.3.9. Отказать в регистрации Оператора СЦИ до получения надлежащим образом (в соответствии с Приложением № 8 к Регламенту) оформленного заявления на подключение Стороннего центра идентификации Уполномоченной организации или в случае ненадлежащего оформления заявления на регистрацию Оператора СЦИ в соответствии с Приложением № 9 к Регламенту.

5.3.10. Отказать в предоставлении доступа к СЭП Пользователям СЭП, не прошедшим многофакторную аутентификацию.

5.3.11. Отказать в предоставлении сведений, а также отказаться от участия в работе разрешительной комиссии по запросу Уполномоченной организации для разбора конфликтной ситуации, связанной с применением электронной подписи, созданной без использования СЭП.

5.3.12. В случае отсутствия подключения к СЭП SMS-шлюза на согласованных с Уполномоченной организацией условиях может осуществляться информирование и аутентификацию Пользователей СЭП посредством отправки информационных сообщений на номер мобильного телефона Пользователя СЭП при выполнении операций в СЭП от имени Пользователя СЭП в соответствии с параметрами настройки СЭП, установленными Уполномоченной организацией по форме в соответствии с Приложением № 6 к Регламенту.

Номер мобильного телефона Пользователя СЭП должен быть зарегистрирован Оператором СЭП в СЭП или передаваться в СЭП Уполномоченной организацией при аутентификации Пользователя СЭП в СЭП.

5.4. Уполномоченная организация имеет право:

5.4.1. Осуществлять с использованием Прикладного интерфейса СЭП подключение собственных Информационных систем к СЭП для получения доступа к функциям создания и проверки электронной подписи, формирования запросов на создание и управление сертификатами ключей проверки электронной подписи, создания и хранения ключей электронной подписи Пользователей СЭП.

5.4.2. Подать Исполнителю заявление на Подключение Оператора СЭП по форме в соответствии с Приложением № 1 к Регламенту и в порядке, установленном п.8.1 Регламента.

5.4.3. Подключить к СЭП SMS-шлюз в соответствии с п. 8.5 настоящего Регламента для отправки Пользователям СЭП информационных сообщений с одноразовыми паролями и уведомлениями о выполняемых СЭП операциях с использованием принадлежащих им ключей ЭП.

5.4.4. Подключать к СЭП собственные Сторонние центры идентификации в соответствии с п. 8.6 настоящего Регламента для управления доступом Пользователей СЭП и Операторов СЦИ к СЭП.

5.4.5. Подать Исполнителю заявление на регистрацию в СЭП Оператора СЦИ по форме в соответствии с Приложением № 9 к Регламенту и в порядке, установленном п.8.6 Регламента.

5.4.6. Подключать к СЭП Удостоверяющие центры в соответствии с п.8.7 настоящего Регламента для автоматической отправки сформированных запросов на создание и управление Сертификатами Пользователей СЭП, получения и установки в СЭП созданных Сертификатов СЭП. СЭП позволяет подключение Удостоверяющих центров, функционирующих на базе ПАК «КриптоПро УЦ» версии 1.5 или версии 2.0.

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

5.4.8. Осуществлять посредством Прикладного интерфейса СЭП выгрузку системных журналов аудита операций, совершаемых Пользователями СЭП при получении доступа к СЭП.

5.4.9. Делегировать Пользователям СЭП право формирования запросов на создание и управление своими Сертификатами посредством Веб- или Прикладного интерфейса СЭП с отправкой их в подключенный Удостоверяющий центр. Предоставленные Уполномоченной организацией права Пользователей СЭП определяются параметрами функционирования СЭП в соответствии с Приложением № 6 к Регламенту и Регламентом деятельности Уполномоченной организации. Уполномоченная организация несет всю полноту своих обязанностей и ответственности за формируемые запросы по заявкам Пользователей СЭП в соответствии с предоставленными им Уполномоченной организацией правами.

5.4.10. Обращаться к доступным из СЭП Службам актуальных статусов сертификатов и штампов времени, технически совместимых со средствами СЭП.

5.4.11. Обратиться к Исполнителю для получения сведений, а также для участия Исполнителя в разрешительной комиссии для разбора конфликтной ситуации, связанной с применением электронной подписи, созданной с использованием СЭП.

5.4.12. Оператор СЭП имеет право:

5.4.12.1. Подключать Пользователей к СЭП, регистрировать и удалять Пользователей СЭП.

5.4.12.2. Формировать запросы на создание Сертификатов Пользователей СЭП.

5.4.12.3. Формировать запросы на приостановление, возобновление и прекращение действия Сертификатов Пользователей СЭП.

5.4.13. Подать Исполнителю заявление на регистрацию Сертификата Оператора СЭП по форме в соответствии с Приложением № 3 к Регламенту и в порядке, установленном п.8.2 Регламента.

6. Ответственность сторон

6.1. Исполнитель не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Исполнитель обоснованно полагался на сведения, указанные в заявлениях и документах, исходящих от Уполномоченной организации.

6.2. Исполнитель несет ответственность за убытки при использовании ключа электронной подписи Пользователя СЭП и Сертификата Пользователя СЭП только в случае, если данные убытки возникли при нарушении конфиденциальности ключа электронной подписи Пользователя СЭП и нарушение конфиденциальности ключа произошла по вине Исполнителя.

6.3. Вся ответственность по занесению данных в запросы на создание Сертификатов Пользователей СЭП, принятию решений по созданию и управлению Сертификатами Пользователей СЭП полностью возлагается на Уполномоченную организацию.

6.4. Вся ответственность по достоверной аутентификации и управлению доступом Пользователей СЭП при использовании стороннего центра идентификации и (или) SMS-шлюза полностью возлагается на Уполномоченную организацию.

6.5. Вся ответственность по подключению Информационных систем Уполномоченной Организации к СЭП полностью возлагается на Уполномоченную организацию.

6.6. Вся ответственность по подключению Удостоверяющего центра к СЭП полностью возлагается на Уполномоченную организацию.

6.7. Ответственность Сторон, не урегулированная положениями настоящего Регламента, устанавливается Договором и законодательством Российской Федерации.

7. Персональные данные

7.1. В целях надлежащего и своевременного оказания комплекса услуг, связанных с предоставлением доступа к СЭП, Исполнитель осуществляет обработку персональных данных Операторов СЭП и Пользователей СЭП в течение срока действия Договора.

7.2. Персональные данные Операторов СЭП и Пользователей СЭП, содержащиеся в документах, предоставляемых Уполномоченной организацией в рамках Договора и в соответствии с настоящим Регламентом, не являются тайной частной жизни, личной и (или) семейной тайной субъектов персональных данных.

7.3. Уполномоченная организация подтверждает и гарантирует, что ею получены письменные согласия Операторов СЭП и Пользователей СЭП по форме Приложения № 12 к настоящему Регламенту, и что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых они являются, относятся к общедоступным персональным данным. Уполномоченная организация несет все неблагоприятные последствия, связанные с неполучением Уполномоченной организацией письменных согласий на обработку персональных данных Исполнителем.

7.4. Исполнителю доступны для обработки общедоступные персональные данные (которые заносятся в сертификат ключа проверки электронной подписи Оператора СЭП и Пользователя СЭП), а именно: фамилия, имя, отчество; СНИЛС; ИНН; адрес места регистрации (страна, субъект РФ, населенный пункт, улица, номер дома, корпуса, строения, квартиры); адрес электронной почты; в том числе номер телефона.

7.5. Требования к защите обрабатываемых персональных данных, в том числе необходимые правовые, организационные и технические меры по защите персональных данных Операторов СЭП и Пользователей СЭП от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении персональных данных определяются Исполнителем самостоятельно с учетом требований законодательства Российской Федерации в области персональных данных и в соответствии с локальными актами Исполнителя.

8. Порядок оказания услуг, связанных с предоставлением доступа к СЭП

8.1. Подключение Оператора СЭП к СЭП

Подключение Оператора СЭП к СЭП осуществляется на основании заявления на регистрацию Оператора СЭП. Форма заявления на регистрацию Оператора СЭП приведена в Приложении № 1 к настоящему Регламенту.

Вместе с заявлением на регистрацию должен быть предоставлен Сертификат Оператора СЭП в электронной форме файл формата X.509 (с расширением .cer) в кодировке DER.

Предоставленный Сертификат Оператора СЭП должен соответствовать следующим требованиям:

1. Принадлежать Уполномоченной организации и содержать сведения о регистрируемом Операторе СЭП (как минимум - фамилия, имя и отчество (если имеется));
2. Сертификат Оператора СЭП должен быть действительным на момент подачи заявления на сертификацию (не содержаться в списках отозванных сертификатах);
3. Срок окончания действия Сертификата Оператора СЭП и соответствующего ключа электронной подписи должен наступать не менее, чем через 3 (три) месяца после даты подачи заявления на регистрацию Оператора СЭП.
4. Ключ проверки электронной подписи, содержащийся в Сертификате Оператора СЭП, должен быть создан с использованием сертифицированного средства электронной подписи, совместимым со средствами СЭП.
5. Адрес электронной почты и прочие сведения, указанные в заявлении на регистрацию Оператора СЭП, должен совпадать со сведениями, содержащимся в предоставленном Сертификате Оператора СЭП, и соответствовать сведениям, полученным от Уполномоченной организации в соответствии с разделом 4 настоящего Регламента.

Предоставление заявительных документов для регистрации Оператора СЭП может быть осуществлено:

- Оператором СЭП;
- Представителем Уполномоченной организации на основании доверенности, оформленной по форме Приложения № 2 к настоящему Регламенту;
- Путем направления корреспонденции курьерской службой доставки или почтой России.

Администратор СЭП проверяет корректность заполнения полученного заявления и достоверности содержащихся в заявлении данных и принимает решение о регистрации Оператора СЭП или отказе в регистрации.

После осуществления регистрации Оператора СЭП Администратор СЭП сообщает Оператору СЭП секретную ключевую фразу и предоставляет параметры настройки функционирования СЭП, включающие URL-адреса подключения к СЭП Оператора СЭП и Пользователей СЭП, Информационных систем и прочие данные в соответствии с Приложением № 6 к Регламенту. Информация может быть отправлена на адрес электронной почты, указанный в заявлении на регистрацию Оператора СЭП, и зашифрована в ключе проверки электронной подписи, содержащимся в предоставленном с заявлением Сертификате СЭП.

Регистрация Оператора СЭП в случае принятия положительного решения должна быть осуществлена в течение одного рабочего дня с даты предоставления заявительных документов на регистрацию Оператора СЭП.

В случае отказа в регистрации Администратор СЭП в течение одного рабочего дня с даты предоставления заявительных документов на регистрацию Оператора СЭП сообщает заявителю о причинах отказа.

Подключение одного Оператора СЭП осуществляется сроком на 1 (один) год в соответствии с условиями Договора.

8.2. Регистрация нового Сертификата Оператора СЭП

При необходимости регистрации нового Сертификата Оператора СЭП (в случае скорого наступления или уже наступившего срока окончания действия сертификата Оператора СЭП, досрочного прекращения действия сертификата Оператора СЭП и т.п.) Оператор СЭП для получения доступа к СЭП подает заявление на регистрацию нового Сертификата Оператора СЭП по форме в соответствии с Приложением № 3 к Регламенту.

При регистрации в СЭП нового Сертификата Оператора СЭП старый Сертификат этого Оператора СЭП удаляется и доступ к СЭП с использованием старого Сертификата Оператора СЭП прекращается.

Вместе с заявлением на регистрацию Сертификата Оператора СЭП должен быть предоставлен сертификат ключа проверки электронной подписи в электронной форме файл формата X.509 (с расширением .cer) в кодировке DER, соответствующий требованиям к Сертификату Оператора СЭП, приведенным в п.8.1 настоящего Регламента.

8.3. Прекращение доступа Оператора СЭП к СЭП

Исполнитель прекращает доступ Оператора СЭП к СЭП в следующих случаях:

- по заявлению Оператора СЭП;
- по заявлению Уполномоченной организации;
- в случае прекращения (приостановления) действия Сертификата Оператора СЭП;
- по истечении срока действия ключа электронной подписи, соответствующего Сертификату Оператора СЭП;
- при прекращении действия настоящего Регламента и (или) Договора в отношении Уполномоченной организации;
- по решению Исполнителя;

В случае прекращения действия настоящего Регламента и (или) Договора Исполнитель должен официально уведомить Оператора СЭП о прекращении доступа к СЭП не позднее одного рабочего дня с момента наступления описанного события.

Официальное уведомление о факте и причине прекращения доступа Оператора СЭП к СЭП направляется в форме электронного письма по адресу электронной почты, указанному в Сертификате Оператора СЭП.

8.3.1. Прекращение доступа Оператора СЭП к СЭП по заявлению Оператора СЭП

Подача заявления на прекращение доступа к СЭП осуществляется Оператором СЭП посредством почтовой или курьерской связи по форме Приложения № 4 к Регламенту.

Заявление также может быть подписано с использованием действующего Сертификата Оператора СЭП и выслано на адрес электронной почты Исполнителя, указанный в разделе 1 настоящего Регламента. В этом случае Оператор СЭП должен убедиться в получении Исполнителем отправленного письма, обратившись по указанному в разделе 1 Регламента телефонному номеру.

После получения Исполнителем заявления на прекращение доступа Оператора СЭП к СЭП Администратор СЭП осуществляет его рассмотрение и обработку. Обработка заявления на прекращение доступа к СЭП должна быть осуществлена не позднее одного рабочего дня, следующего за рабочим днем, в котором указанное заявление было принято Исполнителем.

В случае отказа в прекращении доступа к СЭП Исполнитель уведомляет об этом Оператора СЭП путем направления электронного письма по адресу электронной почты, указанному в Сертификате Оператора СЭП.

При принятии положительного решения Администратор СЭП прекращает доступ Оператора СЭП к СЭП.

8.3.2. Прекращение доступа Оператора СЭП к СЭП по заявлению Уполномоченной организации

Уполномоченная организация вправе прекратить доступ к СЭП своих полномочных представителей – Операторов СЭП, путем подачи заявления по форме, приведенной в Приложении № 4 к настоящему Регламенту (в этом случае подпись Оператора СЭП не требуется).

После получения Исполнителем заявления Уполномоченной организации на прекращение доступа Оператора СЭП к СЭП Администратор СЭП осуществляет его рассмотрение и обработку. Обработка заявления на прекращение доступа Оператора СЭП к СЭП должна быть осуществлена не позднее одного рабочего дня, следующего за рабочим днем, в котором указанное заявление было принято Исполнителем.

В случае отказа в прекращении доступа к СЭП Исполнитель уведомляет об этом Уполномоченную организацию путем направления электронного письма по адресу электронной почты, указанному Уполномоченной организацией в Договоре.

При принятии положительного решения Администратор СЭП прекращает доступ Оператора СЭП к СЭП.

8.3.3. Прекращение доступа Оператора СЭП к СЭП по прекращению (приостановлению) действия Сертификата Оператора СЭП и истечению срока действия соответствующего ключа электронной подписи.

В случае прекращения (приостановления) действия Сертификата Оператора СЭП или истечения срока действия соответствующего ключа электронной подписи доступ Оператора СЭП к СЭП прекращается автоматически. Уведомление Оператору СЭП о прекращении доступа в этом случае не высылаются.

Для получения (восстановления) доступа Оператор СЭП к СЭП должен зарегистрировать свой новый Сертификат Оператора СЭП в соответствии с п. 8.2. настоящего Регламента.

8.3.4. Прекращение доступа Оператора СЭП к СЭП по решению Исполнителя

Исполнитель вправе прекратить доступ Оператора СЭП к СЭП в случаях нарушения конфиденциальности и (или) подозрения в нарушении конфиденциальности аутентификационных данных, если Оператору СЭП не было известно о возможном факте нарушения конфиденциальности, а также в случаях неисполнения Оператором СЭП условий Договора и настоящего Регламента.

После прекращения доступа Оператора СЭП к СЭП Администратор СЭП сообщает Оператору СЭП о наступлении события, повлекшего прекращение доступа, и уведомляет его о том, что доступ Оператора СЭП к СЭП прекращен с указанием причин, повлекших прекращение доступа, путем направления электронного письма по адресу электронной почты, указанному в Сертификате Оператора СЭП.

Восстановление доступа Оператора к СЭП осуществляется Администратором СЭП в течение одного рабочего дня после устранения причин, повлекших прекращение доступа Оператора СЭП к СЭП, и получения Исполнителем уведомления об этом.

8.4. Подключение Информационной системы Уполномоченной организации к СЭП

Исполнитель предоставляет Уполномоченной организации Прикладной интерфейс подключения к СЭП в соответствии с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика». Защита передаваемых от Информационной

системы к СЭП данных осуществляется в соответствии с требованиями Уполномоченной организации с использованием СКЗИ, совместимых со средствами СЭП.

Адреса подключения Информационных систем указываются в таблице параметров настройки функционирования СЭП по форме, приведенной в Приложении № 6 к Регламенту, и предоставляемой Уполномоченной организации при регистрации первого Оператора СЭП.

В случае необходимости изменения параметров настройки функционирования СЭП Уполномоченная организация после предварительного согласования в рабочем порядке направляет Исполнителю подписанный исправленный вариант параметров настройки СЭП по форме в соответствии с Приложением № 6 к Регламенту.

8.5. Подключение SMS-шлюза Уполномоченной организации к СЭП

Подключение SMS-шлюза Уполномоченной организации к СЭП осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению Уполномоченной организации по форме в соответствии с Приложение № 7 к Регламенту. Заявление передается в Исполнителю курьерской или почтовой связью.

Заявление на подключение SMS-шлюза может быть отправлено Администратору СЭП в электронной форме, подписано электронной подписью Оператора СЭП и руководителя Уполномоченной организации, с обязательной последующей передачей оригинала заявления на бумажном носителе.

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 № 7 к Регламенту.

Защита передаваемых от СЭП на SMS-шлюз Уполномоченной организации информационных сообщений осуществляется в соответствии с требованиями Уполномоченной организации с использованием СКЗИ, совместимых со средствами СЭП.

8.6. Подключение Стороннего центра идентификации Уполномоченной организации к СЭП

Подключение СЦИ к СЭП осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению Уполномоченной организации по форме в соответствии с Приложение № 8 к Регламенту. Заявление передается Исполнителю курьерской или почтовой связью. Вместе с заявлением на носителе информации передается сертификат СЦИ, используемый для проверки идентификационной информации, получаемой СЭП от Стороннего центра идентификации.

Настройка параметров СЭП для подключения СЦИ осуществляется в течение 5 (пяти) рабочих дней с даты получения Исполнителем подписанного заявления по форме в соответствии с Приложение № 8 к Регламенту.

СЦИ подключается сроком на 1 (один) год в соответствии с условиями Договора.

В случае смены сертификата СЦИ Уполномоченная организация осуществляет повторное подключение СЦИ в соответствии с настоящим пунктом.

Заявление на подключение и сертификат СЦИ могут быть отправлены Администратору СЭП в электронной форме, подписано электронной подписью Оператора СЭП и руководителя Уполномоченной организации, с обязательной последующей передачей оригинала заявления на бумажном носителе.

Регистрация Оператора СЦИ в СЭП выполняется после получения заявления по форме в соответствии с Приложением № 9 к Регламенту. Заявление передается Исполнителю курьерской или почтовой связью.

Заявление на регистрацию Оператора СЦИ может быть отправлено Администратору СЭП в электронной форме, подписано электронной подписью Оператора СЭП и руководителя Уполномоченной организации, с обязательной последующей передачей оригинала заявления на бумажном носителе.

8.7. Подключение Удостоверяющего центра к СЭП

Подключение УЦ к СЭП заключается в установлении сетевого взаимодействия компонент СЭП со средствами автоматизации деятельности УЦ, предназначено для непосредственной автоматической передачи из СЭП в УЦ формируемых запросов на создание сертификатов и управление ими (приостановление, возобновление и прекращение действия сертификатов) и осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению Уполномоченной организации по форме в соответствии с Приложение № 10 к Регламенту. Заявление передается Исполнителю курьерской или почтовой связью. Вместе с заявлением на носителе информации передается Сертификат Удостоверяющего центра, используемый для подключения СЭП к УЦ.

Уполномоченная организация за свой счет обеспечивает получение Исполнителем ключа ЭП и Сертификата СЭП для подключения к УЦ в соответствии с установленным порядком деятельности УЦ или применение имеющегося у Исполнителя Сертификата СЭП для подключения к УЦ.

Подключение УЦ возможно только в случае использования средств автоматизации деятельности УЦ на базе ПАК «КриптоПро УЦ» версий 1.5 или 2.0, доступных с использованием сети Интернет.

Защита передаваемых от СЭП в УЦ информации осуществляется в соответствии с требованиями УЦ с использованием СКЗИ, совместимых со средствами СЭП.

Настройка параметров СЭП для подключения УЦ осуществляется в течение 5 (пяти) рабочих дней с даты получения Исполнителем подписанного заявления по форме в соответствии с Приложение № 10 к Регламенту.

Настройку средств УЦ для подключения к СЭП обеспечивает Уполномоченная организация.

УЦ подключается к СЭП сроком на 1 (один) год в соответствии с условиями Договора.

В случае прекращения действия Сертификата Удостоверяющего центра, использованного для подключения УЦ к СЭП, Уполномоченная организация осуществляет повторное подключение УЦ в соответствии с настоящим пунктом.

Заявление на подключение УЦ и необходимый для подключения УЦ Сертификат Удостоверяющего центра могут быть отправлены Администратору СЭП в электронной форме, подписано электронной подписью Оператора СЭП и руководителя Уполномоченной организации, с обязательной последующей передачей оригинала заявления на бумажном носителе.

8.8. Регистрация Пользователей СЭП, формирование запросов на создание и управление Сертификатами Пользователей СЭП, управление доступом Пользователей СЭП к СЭП

Регистрация Пользователей СЭП, формирование запросов на создание и управление Сертификатами Пользователей СЭП производится Оператором СЭП и осуществляется в соответствии с порядком, установленным Уполномоченной организацией.

СЭП реализует функции по регистрации и аутентификации Пользователей СЭП, формированию запросов на создание Сертификатов Пользователей СЭП, прекращение действия Сертификатов Пользователей СЭП, приостановление и возобновление действия Сертификатов Пользователей СЭП в соответствии с параметрами настройки функционирования СЭП, предоставленных Исполнителем и согласованных с Уполномоченной организацией по форме в соответствии с Приложением № 6 к Регламенту.

Перечисленные выше функции СЭП выполняются на основании заявок в электронном виде внутреннего формата СЭП, направляемых Оператором СЭП и (или) Пользователями СЭП посредством Веб- или Прикладного интерфейса СЭП, при следующих условиях:

- Подтвержден уникальный идентификатор Центра идентификации СЭП или Стороннего центра идентификации Уполномоченной организации, в котором зарегистрирован Оператор СЭП и (или) Пользователь СЭП;
- Сертификат Оператора СЭП на момент получения заявки в СЭП действителен или идентификатор Оператора СЭП получен от Стороннего центра идентификации.
- Аутентификация Пользователя СЭП подтверждена с помощью HMAC или одноразовым паролем, переданного заявителю от СЭП посредством информационного сообщения или сформированным им с использованием OTP-токена, полученного от Оператора СЭП.

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

Доступ Пользователей СЭП к СЭП осуществляется посредством Веб- или Прикладного интерфейса СЭП, на основании аутентификационной информации, переданной Уполномоченной организацией при регистрации и подключении Пользователя СЭП к СЭП или полученной от Стороннего центра идентификации.

Функции создания ЭП с использованием СЭП доступны Пользователям СЭП при выполнении следующих условий:

1. Пользователь СЭП является владельцем действующего Сертификата Пользователя СЭП, соответствующий которому ключ ЭП создан с использованием СЭП;
2. Сертификат Пользователя СЭП зарегистрирован в СЭП Уполномоченной организацией.
3. Сертификат Удостоверяющего центра, создавшего Сертификат Пользователя СЭП, передан Администратору и установлен в СЭП.
4. Список отозванных сертификатов Пользователя СЭП, созданных УЦ, актуален и доступен для СЭП по сетевому адресу (url), содержащемуся в Сертификате Пользователя СЭП (значение CRL Distribution Point).

Пользователь СЭП подтверждает использование своего ключа ЭП посредством ввода индивидуального ПИН-кода доступа к ключу ЭП и применения HMAC или ввода одноразового пароля, формируемого СЭП и отправляемого в информационном сообщении на номер мобильного телефона, указанный при регистрации Пользователя СЭП. Одноразовый пароль для подтверждения операций с ключом ЭП может быть сформирован OTP-токеном, выдаваемым Оператором СЭП по заявлению Пользователя СЭП.

Срок предоставления Пользователю доступа к СЭП определяется условиями Договора.

8.9. Применение Служб актуальных статусов сертификатов и штампов времени при использовании СЭП

При создании и проверке ЭП усовершенствованного формата криптографических сообщений (CAdES-T, CAdES-X Long Type 1) СЭП использует Службу актуальных статусов сертификатов Удостоверяющего центра, доступную по сетевому адресу (url), содержащемуся в Сертификате Пользователя СЭП (значение Authority Information Access), с использованием которого создается ЭП, и Службу штампов времени, доступную по сетевому адресу (url), содержащемуся в запросе на создание ЭП, передаваемому в СЭП с использованием Прикладного интерфейса СЭП. Для применения Службы штампов времени с использованием Веб-интерфейса СЭП адрес и наименование этой службы должны быть указаны в предоставляемых Уполномоченной организацией параметрах настройки СЭП в соответствии с Приложением № 6 к Регламенту.

8.10. Участие Исполнителя в экспертизе электронной подписи

По запросу Уполномоченной организации Исполнитель участвует в проведении экспертных работ для разбора конфликтной ситуации в отношении электронной подписи, созданной с использованием СЭП, и предоставляет информацию из журналов аудита СЭП, необходимую для разрешения конфликтной ситуации.

Для получения необходимых сведений Уполномоченная организация подает заявление Исполнителю по форме, приведенной в Приложении № 11 к Регламенту.

Заявление должно содержать следующую информацию:

- дата подачи заявления;
- идентификационные данные Пользователя СЭП, информацию о создании ЭП или ключа ЭП которого необходимо предоставить;
- время и дата формирования ЭП или ключа ЭП;
- перечень сведений, которые необходимо предоставить.

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

- сертификат ключа проверки электронной подписи, с использованием которого создана ЭП, в отношении которой производится разбор конфликтной ситуации.

Организацию работы разрешительной комиссии по разбору конфликтной ситуации осуществляет Уполномоченная организация.

В срок не более 10 (десяти) рабочих дней с даты получения заявления Исполнитель предоставляет Уполномоченной организации отчет, включающий запрошенные сведенья, и в рабочем порядке согласует участие в мероприятиях, проводимых разрешительной комиссией.

Отчет Исполнителя составляется в произвольной форме, подписывается Администратором СЭП и руководителем, заверяется печатью Исполнителя и предоставляется Уполномоченной организации.

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

9.1. Структура запроса на создание сертификата Пользователя СЭП

СЭП формирует запросы на создание Сертификатов Пользователей СЭП в соответствии со стандартом PKCS - PKCS#10.

Ключи ЭП Пользователей СЭП создаются с использованием сертифицированного Средства ЭП ПАКМ «КриптоПро HSM» по алгоритму ГОСТ Р 34.10-2001.

9.2. Сроки действия ключевых документов

9.2.1. Срок действия ключа ЭП Пользователя СЭП составляет 15 (пятнадцать) месяцев.

9.2.2. Срок действия ключа проверки ЭП Пользователя СЭП составляет не более 15 (пятнадцати) лет.

9.2.3. Начало периода действия ключей ЭП Пользователя СЭП исчисляется с даты и времени формирования запроса на создание Сертификата Пользователя СЭП.

9.2.4. Использование ключа ЭП после окончания срока его действия не допускается.

10. Дополнительные положения

10.1. Нарушение конфиденциальности ключевых документов Пользователя СЭП

Пользователь СЭП самостоятельно принимает решение о факте и (или) угрозе нарушения конфиденциальности своего ключа ЭП.

В случае нарушения конфиденциальности и (или) угрозы нарушения конфиденциальности ключа ЭП Пользователь СЭП прекращает или приостанавливает действие своего Сертификата Пользователь СЭП в соответствии с порядком, установленным Удостоверяющим центром, создавшим этот Сертификат Пользователь СЭП, или Уполномоченной организацией.

10.2. Конфиденциальность информации

10.2.1. Типы конфиденциальной информации

10.2.1.1. Ключ ЭП, соответствующий Сертификату Пользователя СЭП, является конфиденциальной информацией лица, зарегистрированного в СЭП. В СЭП не осуществляется хранение ключей ЭП Пользователей СЭП. Пользователи СЭП хранят свои ключи ЭП с использованием СЭП.

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

10.2.1.3. 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.

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

10.2.2. Типы информации, не являющейся конфиденциальной

10.2.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой (общедоступной) информацией.

10.2.2.2. Открытая информация может публиковаться по решению Исполнителя. Место, способ и время публикации открытой информации определяется Исполнителем.

10.2.2.3. Информация, включаемая в запросы на создание Сертификатов Пользователей СЭП, формируемые в СЭП, не считается конфиденциальной.

10.2.2.4. Персональные данные, включаемые в запросы на создание Сертификатов Пользователей СЭП, формируемые в СЭП, относятся к общедоступным персональным данным.

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

10.2.3. Исключительные полномочия Исполнителя

10.2.3.1. Исполнитель имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

10.3. Хранение информации в СЭП

Срок хранения журналов аудита операций, совершаемых в СЭП, составляет 5 (пять) лет с момента выполнения операций.

Срок хранение резервных копий данных, создаваемых в СЭП, составляет 1 (один) год.

Регистрационная или идентификационная информация, ключи ЭП, запросы на создание Сертификатов Пользователей СЭП и зарегистрированные Сертификаты

Пользователей СЭП удаляются в момент удаления их Оператором СЭП или Пользователем СЭП.

В случае прекращения действия настоящего Регламента в отношении Уполномоченной организации вся информация о Пользователях СЭП, зарегистрированных этой Уполномоченной организацией, удаляется.

10.4. Прекращение оказания комплекса услуг, связанных с предоставлением доступа к СЭП

10.4.1. В случае прекращения действия Договора и настоящего Регламента в отношении Уполномоченной организации вся информация в СЭП о Пользователях СЭП, зарегистрированных этой Уполномоченной организацией, в том числе ключи ЭП, запросы на создание Сертификатов и зарегистрированные Сертификаты Пользователей СЭП, удаляется. От СЭП отключаются все Операторы СЭП, СЦИ, УЦ и SMS-шлюз Уполномоченной организации.

11. Список приложений

11.1. Приложение № 1. Форма заявления на регистрацию Оператора СЭП.

11.2. Приложение № 2. Форма доверенности на предоставление заявительных документов для подключения Оператора СЭП.

11.3. Приложение № 3. Форма заявления на регистрацию Сертификата Оператора СЭП..

11.4. Приложение № 4. Форма заявления на прекращение доступа Оператора СЭП.

11.5. Приложение № 5. Функции Сервиса электронной подписи.

11.6. Приложение № 6. Форма перечня параметров настройки функционирования СЭП.

11.7. Приложение № 7. Форма заявления на подключение SMS-шлюза..

11.8. Приложение № 8. Форма заявления на подключение Стороннего центра идентификации.

11.9. Приложение № 9. Форма заявления на регистрацию Оператора СЦИ.

11.10. Приложение № 10. Форма заявления на подключение Удостоверяющего центра.

11.11. Приложение № 11. Форма запроса на предоставление информации для разбора конфликтной ситуации.

11.12. Приложение № 12. Форма письменного согласия субъекта персональных данных.

Приложение №1 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма заявления на регистрацию Оператора СЭП)

Заявление на регистрацию Оператора Сервиса электронной подписи 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 Сервисе электронной подписи ООО «КРИПТО-ПРО» и наделить полномочиями Оператора СЭП ООО «КРИПТО-ПРО», установленными Регламентом Сервиса электронной подписи ООО «КРИПТО-ПРО».

Идентификационные данные Оператора СЭП:

Фамилия, Имя и Отчество (если имеется) полномочного представителя – Оператора СЭП	
Логин полномочного представителя – Оператора СЭП (латинские буквы и цифры)	
Наименование Уполномоченной организации	
Номер Сертификата Оператора СЭП Оператора СЭП	
Отпечаток (Хеш sha1) Сертификата Оператора СЭП	
Адрес электронной почты Оператора СЭП	
ИНН Уполномоченной организации (указывается, если содержится в предоставленном Сертификате Оператора СЭП)	
ОГРН Уполномоченной организации (указывается, если содержится в предоставленном Сертификате Оператора СЭП)	

Сертификат Оператора СЭП в электронной форме прилагается.

Настоящим _____
(фамилия, имя, отчество)

соглашается с обработкой своих персональных данных ООО «КРИПТО-ПРО» в целях идентификации для предоставления доступа к СЭП и признает, что персональные данные, указанные в сертификате ключа проверки 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 №2 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма доверенности на предоставление заявительных
документов Оператора СЭП)

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 ООО «КРИПТО-ПРО» необходимые документы, определенные Регламентом Сервиса электронной подписи ООО «КРИПТО-ПРО» для регистрации своего полномочного представителя - Оператора СЭП ООО «КРИПТО-ПРО»

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

Представитель наделяется правом расписываться в соответствующих документах ООО «КРИПТО-ПРО» для исполнения поручений, определенных настоящей доверенностью.

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

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

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

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

«___»_____20__ г.

М.П.

Приложение №3 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма заявления на регистрацию Сертификата Оператора СЭП)

Заявление на регистрацию сертификата ключа проверки электронной подписи Оператора Сервиса электронной подписи ООО «КРИПТО-ПРО»

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит зарегистрировать сертификат ключа проверки электронной подписи своего уполномоченного представителя – Оператора СЭП ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными:

Фамилия, Имя и Отчество (если имеется) полномочного представителя – Оператора СЭП	
Логин полномочного представителя – Оператора СЭП (латинские буквы и цифры)	
Наименование Уполномоченной организации	
Номер Сертификата Оператора СЭП Оператора СЭП	
Отпечаток (Хеш sha1) Сертификата Оператора СЭП	
Адрес электронной почты Оператора СЭП	
ИНН Уполномоченной организации (указывается, если содержится в предоставленном Сертификате Оператора СЭП)	
ОГРН Уполномоченной организации (указывается, если содержится в предоставленном Сертификате Оператора СЭП)	

Сертификат Оператора СЭП в электронной форме прилагается.

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

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

«___»_____20__ г.

М.П.

Приложение № 4 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма заявления на прекращение доступа Оператора СЭП)

Заявление на прекращение доступа Оператора СЭП 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 прекращения доступа)

Просит прекратить доступ своего уполномоченного представителя – Оператора СЭП ООО «КРИПТО-ПРО»: _____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Фамилия, Имя и Отчество (если имеется) полномочного представителя – Оператора СЭП	
Логин полномочного представителя – Оператора СЭП (латинские буквы и цифры)	
Наименование Уполномоченной организации	
ИНН Уполномоченной организации (указывается, если содержится в предоставленном Сертификате Оператора СЭП)	
ОГРН Уполномоченной организации (указывается, если содержится в предоставленном Сертификате Оператора СЭП)	

Оператор СЭП _____ /_____/
Подписывает в случае подачи заявления от Оператора СЭП (подпись) (фамилия, инициалы)
«___»_____20__ г.

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

«___»_____20__ г.

М.П.

Приложение №5 к Регламенту Сервиса электронной подписи
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 СЭП.
2. Создания и проверки электронной подписи электронных документов различного формата криптографических сообщений.
3. Формирование запросов на создание и управление Сертификатами Пользователей СЭП
4. Взаимодействия Операторов и Пользователей СЭП с Удостоверяющим центром для передачи запросов на создание и управления Сертификатами Пользователей СЭП, получения и установки в СЭП полученных сертификатов для дальнейшего использования при создании электронной подписи. СЭП позволяет непосредственное взаимодействие с Удостоверяющим центром на базе ПАК «КриптоПро УЦ» версий 1.5 или 2.0.

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, CAdES-T 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 СЭП, 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) или Auth2.0 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 СЭП в информационном сообщении или формируемого с помощью OTP-токена, или с использованием HMAC.

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

5. Информирование Пользователей Удостоверяющего центра

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

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 СЭП.

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

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

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 Пользователем СЭП 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 Удостоверяющим центром, подключенным к СЭП или к Информационной системе Уполномоченной организации.

Использование ключа электронной подписи в СЭП должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем СЭП) с помощью HMAC или одноразового пароля, формируемого

персональным OTP-токеном владельца сертификата ключа проверки электронной подписи или высылаемого в информационном сообщении на указанный при регистрации Пользователем СЭП мобильный телефон владельца сертификата ключа электронной подписи Пользователя СЭП, а также индивидуальным PIN-кодом доступа к ключевому контейнеру, содержащему используемый ключ электронной подписи.

Пользователь СЭП 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 СЭП обязан немедленно обратиться к Оператору СЭП 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 СЭП стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе если Пользователь СЭП получил сообщение от СЭП о выполнении каких-либо операций от его имени в то время, когда он их не выполнял.

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

8. Аудит Сервиса электронной подписи

Регистрация всех операций, выполняемых Операторами и Пользователями СЭП, 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 № 6 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма перечня параметров настройки функционирования СЭП)

Перечень параметров настройки функционирования Сервиса электронной подписи ООО «КРИПТО-ПРО»

_____
(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:

	Параметр	**Значение параметра**
1.	**Адреса веб-интерфейсов**	
1.1.	URL-адрес веб-интерфейса сервиса подписи	https://www.justsign.me/<company-name>/ или «Не предоставлять»
		Порт доступа (алгоритм шифрования трафика (TLS)): 443 (RSA), 80
1.2.	URL-адрес личного кабинета Пользователей СЭП	https://www.justsign.me/<company-name> idp/users/ или «Не предоставлять»
		Порт доступа (алгоритм шифрования трафика (TLS)): 443 (RSA), 80
1.3.	URL-адрес веб-интерфейса для подключения Оператора СЭП	https://www.justsign.me/< company-name>idp/admins/
		Порт доступа (алгоритм шифрования трафика (TLS)): 443 (RSA), 4430 (ГОСТ)
2.	**Адреса программных интерфейсов**	

2.1.	Базовый URL-адрес[1] Прикладного интерфейса СЭП	**SOAP:** https://www.justsign.me/<company-name>ss/ **REST:** https://www.justsign.me/<company-name>ss/rest/api	
		Порт доступа (алгоритм шифрования трафика (TLS)): 443 (RSA), 80	
2.2.	Базовый URL-адрес Центра идентификации СЭП	https://www.justsign.me/<company-name>idp/ Управление пользователями: https://www.justsign.me/<company-name>idp/ums/ OAuth 2.0: https://www.justsign.me/<company-name>idp/oauth/authorize https://www.justsign.me/<company-name>idp/oauth/token	
		Порт доступа (алгоритм шифрования трафика (TLS)): 443 (RSA), 80	
2.3.	URL-адрес сервиса проверки ЭП	https://www.justsign.me/verifycpc	
2.4	Сетевые адреса (IP) СЭП	Входящий	193.37.157.28
		Исходящий	193.37.157.5
3.	**Настройки СЭП**		
3.1.	Доступные форматы подписи	Оставить требуемые из перечня: 1. «Чистая» ЭП ГОСТ 34.10 – 2001; 2. CAdES-BES/ T/ X Long Type 1; 3. XMLDSig; 4. PDF-CMS/CAdES; 5. MS Office. (по умолчанию - ***Все***)	
3.2.	Использование ПИН-кода для ключевого контейнера	Требовать/Не требовать/Позволять задавать (по умолчанию - ***Позволять задавать***)	
3.3.	Максимальный размер подписываемого документа	5Мб. (по умолчанию – ***5Мб***, ограничение не больше 50Мб)	
3.4.	URL-адрес Службы штампов времени		
4.	**Настройки ЦИ**		
4.1.	Отпечаток сертификата (значение хэш sha1) Центра идентификации СЭП[2]		

[1] Полные адреса конечных точек приведены в ЖТЯИ.00046-02 97 01 «КриптоПро DSS. Руководство разработчика.»

[2] Сертификат ЦИ СЭП необходимо получить у Администратора СЭП

	Профиль пользователя	
4.2.	Состав компонентов имени Пользователя	Выбрать из списка (по умолчанию – все): 1. ОГРН 2. ОГРНИП 3. СНИЛС 4. ИНН 5. Электронная почта 6. Страна 7. Область 8. Город 9. Организация 10. Подразделение 11. Общее имя 12. Адрес 13. Должность 14. Инициалы 15. Имя 16. Фамилия
4.3.	Обязательные для заполнения компоненты имени	Выбрать из представленного списка компонент имени (по умолчанию – ***11.Общее имя***)
4.4.	Значения по молчанию для компонент имени	Выбрать из представленного списка компонент имени (по умолчанию – ***не задано***)
4.5.	Требовать ли уникальность всей совокупности компонент в профиле пользователя	Требовать/Не требовать (по умолчанию – ***не требовать***)
4.6.	Разрешено ли пользователю редактировать свой профиль	Разрешено/запрещено (по умолчанию – ***Разрешено***)
	Политика учетных записей	
4.7.	Используемые идентификаторы пользователя[3]	Логин/Номер телефона/email (по умолчанию – логин)
4.8.	Подтверждение телефона с отправкой СМС (если в качестве идентификатора выбран номер телефона)	Требуется/Не требуется (по умолчанию – ***не требуется***)

[3] Допускается использовать несколько идентификаторов. Если в качестве идентификаторов пользователей используются номера телефона и/или адреса электронной почты, то должна быть обеспечена их уникальность.

4.9.	Подтверждение email с отправкой письма (если в качестве идентификатора выбран адрес электронной почты)	Требуется/Не требуется (по умолчанию – ***не требуется***)
4.10.	Саморегистрация Пользователей СЭП	Разрешена/запрещена (по умолчанию ***Разрешена***)
4.11.	Временная блокировка самостоятельно зарегистрированных пользователей	Да/нет (по умолчанию - ***нет***)
	Настройки первичной аутентификации	
4.12.	Вид первичной аутентификации	По паролю/По сертификату/В СЦИ (по умолчанию – ***по паролю, по сертификату***)
4.13.	Разрешено ли пользователю изменять настройки первичной аутентификации[4]	Разрешено/Запрещено (по умолчанию – ***Запрещено***)
	Парольная аутентификация	
4.14.	Длина долговременных паролей (в символах)	От 1 до 256 (по умолчанию - ***8***)
4.15.	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***)
4.16.	Максимальное количество попыток ввода долговременного пароля до блокирования учетной записи	От 0 до 2147483647, 0 – блокирование отключено (по умолчанию – ***5***)
4.17.	Срок действия пароля в днях	(по умолчанию – ***не ограничено***)
4.19.	Требование смены пароля Пользователя при первом входе[5]	Требовать/Не требовать (по умолчанию – ***не требовать***)
	Настройки вторичной аутентификации	
4.20.	Вторичная аутентификация пользователей	Отключена/Требуется для всех операций/Опционально по списку операций (по умолчанию – ***Отключена***)

[4] Данная настройка имеет значение, только если включено несколько методов первичной аутентификации, но назначать Пользователю тот или иной метод входа должен только Оператор. Данная настройка не запрещает Пользователю менять данные аутентификации - например, сменить пароль или назначить другой сертификат для входа.

[5] Данное правило применяется только в том случае, если учётная запись Пользователя была создана Оператором или пароль Пользователя был сброшен Оператором

4.21.	Список операций требующих подтверждения (в случае выбора вторичная аутентификация пользователей – Опционально)	Выбрать из списка: 1. Выпуск маркера безопасности («вход» Пользователя) 2. Подпись документа 3. Подпись пакета документов 4. Расшифрование документа 5. Создание запроса на сертификат 6. Удаление сертификата 7. Смена пин-кода для доступа к закрытому ключу сертификата 8. Создание запроса на обновление сертификата 9. Создание запроса на отзыв сертификата 10. Создание запроса на приостановление действия сертификата 11. Возобновление действия сертификата
4.22.	Разрешить Пользователю редактирование настроек вторичной аутентификации	Разрешено/Запрещено (по умолчанию ***Разрешено***)
4.23.	Разрешить Оператору редактирование настроек вторичной аутентификации пользователей	Разрешено/Запрещено (по умолчанию ***Разрешено***)
	Одноразовые пароли	
4.24.	Длина одноразовых паролей	От 1 до 256 (по умолчанию – ***5***)
4.25.	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***)
4.26.	Максимальное количество попыток ввода одноразового пароля	От 0 до 2147483647, 0 – блокирование отключено (по умолчанию – ***3***)
4.27.	Максимальное время в секундах, которое предоставляется Пользователю для выполнения операции, подтверждённой одноразовым паролем[6]	(по умолчанию – ***300***)

[6] Период времени, в течение которого Пользователь должен выполнить подтверждённую операцию (подпись, расшифрование документа, создание запроса на сертификат и т.п.). Если в течение данного периода времени Пользователь не выполнил операцию, то потребуется выполнить подтверждение операции повторно.

<table>
<tr><td>4.28.</td><td>Время подтверждения одноразового пароля (в секундах)[7]</td><td colspan="3">(по умолчанию – 300)</td></tr>
<tr><td>4.29.</td><td>Минимальное время (в секундах), в течении которого Пользователь не может запрашивать повторную отправку одноразового пароля[8]</td><td colspan="3">(по умолчанию – 300)</td></tr>
<tr><td>4.30</td><td>Максимальный размер поля с информацией о документе, передаваемой SAML-токене Пользователя (в символах)</td><td colspan="3">От 0 до 256
(по умолчанию 256)</td></tr>
<tr><td>5.</td><td colspan="4">Дополнительно</td></tr>
<tr><td rowspan="4">5.1.</td><td rowspan="4">В случае необходимости разделения пользователей на группы указать имена групп, их описание и назначение оператора.</td><td colspan="3">Опционально. Если не указан – используется группа по умолчанию для всех пользователей.</td></tr>
<tr><td>Имя группы</td><td>Описание</td><td>Логин Оператора группы</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>5.2.</td><td>Политика подтверждения операций для групп пользования (в случае разделения на группы)</td><td colspan="3">Соответствует политикам ЦИ/Назначается для группы[9]
(по умолчанию - Соответствует политикам ЦИ)</td></tr>
<tr><td>5.3.</td><td>Доставлять ключ для myDSS двумя частями (использовать дополнительный код активации по смс или электронной почте)</td><td colspan="3">Требуется/Не требуется
(по умолчанию - Требуется)</td></tr>
<tr><td>6.</td><td colspan="4">Сторонний ЦИ</td></tr>
<tr><td>6.1.</td><td>Режим создания учетных записей в СЭП для пользователей сторонних ЦИ</td><td colspan="3">Автоматический при первом подключении/ Оператором
(по умолчанию – Автоматический)</td></tr>
<tr><td>7.</td><td colspan="4">Взаимодействие с УЦ</td></tr>
<tr><td>7.2.</td><td>Автоматическое создание сертификатов по запросу Пользователей СЭП</td><td colspan="3">Разрешена/Запрещена
(по умолчанию Запрещено)</td></tr>
<tr><td>7.3.</td><td>Автоматическое управление и обновление сертификатов по запросу Пользователей СЭП (при наличии действующего сертификата Пользователей СЭП)</td><td colspan="3">Разрешено/Запрещено
(по умолчанию Запрещено)</td></tr>
</table>

[7] Период времени, в течение которого Пользователь должен подтвердить одноразовый пароль. Если в течение данного периода одноразовый пароль не был подтвержден, то Пользователь должен запросить новый одноразовый пароль для подтверждения. Также в течение этого периода действует счётчик неверных попыток ввода одноразового пароля; при запросе нового одноразового пароля счётчик обнуляется

[8] Интервал времени, через который Пользователь может запросить новый одноразовый пароль. Другими словами, если в течение этого интервала времени Пользователь превысил количество неверных попыток ввода одноразового пароля, то новый пароль он сможет запросить не раньше истечения указанного периода времени

[9] В случае выбора варианта «Назначается для группы», для каждой группы нужно задать политики подтверждения операций аналогично разделу «Настройка вторичной аутентификации»

8.	**Параметры OAuth**	
8.1.	Использовать протокол OAuth 2.0	Да/Нет (по умолчанию – ***нет***)
8.2.	Сценарий использования OAuth	Допустимые значения: ResourceOwner – авторизация с использованием учётных данных пользователя. AuthorizationCode – авторизация с использованием кода авторизации. Implicit – неявная авторизация.
8.3.	Адрес перенаправления redirect_uri *(указывается для сценариев использования OAuth с кодом авторизации (AuthorizationCode) и неявной авторизацией (Implicit))*	URI, по которому ЦИ отправит результат авторизации (типа https://127.0.0.1/oauth/response или urn:oauth-redirect)
8.4.	Идентификатор клиента client_id. (Назначает Исполнитель)	
9.	**Уведомления**	
9.1.	Перечень событий для рассылки уведомлений Пользователям и Операторам СЭП	Указывается в соответствии с таблицей «Типы сообщений с уведомлениями СЭП (по умолчанию).xlsx»  Типы сообщений с уведомлениями СЭ

Дополнительные настройки (кастомизация Web-интерфейса пользователя/оператора, иконка стороннего ЦИ, регистрация специальных OID и шаблонов сертификатов и т.п.) согласовываются с Администратором СЭП.

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

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

«___»_____20__ г.

М.П.

Приложение № 7 к Регламенту Сервиса электронной подписи
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.

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

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

«___»_____20__ г.

М.П.

Приложение № 8 к Регламенту Сервиса электронной подписи
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
2.	Наименование СЦИ	Отображаемое в Web-интерфейсе СЭП имя стороннего ЦИ
3.	Адрес СЦИ	URL-адрес взаимодействия с СЦИ (необходим при web-доступе пользователей)
4.	Краткое описание СЦИ	Краткие сведения о подключаемом СЦИ
5.	Срок действия сертификата СЦИ	Дата начала и окончания действия сертификата Стороннего ЦИ (NotBefore, NotAfter)
6.	Отпечаток сертификата СЦИ	Хеш сертификата СЦИ (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).
9.	ФИО	Работник Уполномоченной Организации, ответственный за подключение и функционирование СЦИ, 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 № 9 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма заявления на регистрацию Оператора СЦИ)

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 СЦИ 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
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)

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

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

М.П.

Приложение № 10 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма заявления на подключение Удостоверяющего центра)

Заявление на подключение Удостоверяющего центра 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 Удостоверяющий центр к Сервису электронной подписи ООО «КРИПТО-ПРО» в соответствии с указанными в настоящем заявлении сведениями:

№ п/п	Параметр СЭП	Настраиваемое значение параметра СЭП
1.	Наименование Удостоверяющего центра	
2.	URL и сетевой (IP) адрес Удостоверяющего центра	URL-адрес Удостоверяющего центра
		Сетевой (IP) адрес и номер порта Удостоверяющего центра
3.	Адреса публикации списков отозванных сертификатов (CDP)	
4.	Адрес публикации порядка деятельности УЦ и получения сертификата для подключения к УЦ	
5.	Контактная информация представителя Уполномоченной организации, ответственного за обеспечение получения Сертификата СЭП для подключения к УЦ	
5.1.	ФИО	
5.2.	Подразделение	
5.3.	Адрес электронной почты	
5.4.	Номер рабочего телефона	

Уполномоченная организация обеспечивает _____
_____
(получение ООО «КРИПТО-ПРО» Сертификата СЭП для подключения к УЦ в соответствии с установленным порядком деятельности УЦ или применение имеющегося у ООО «КРИПТО-ПРО» Сертификата СЭП для подключения к УЦ).

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

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

«___»_____20__ г.

М.П.

Приложение № 11 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма запроса на предоставление информации для разбора конфликтной ситуации)

Запрос информации для разбора конфликтной ситуации

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит предоставить следующие сведения, необходимые для разбора конфликтной ситуации, возникшей в результате применения электронной подписи с использованием Сервиса электронной подписи ООО «КРИПТО-ПРО»:

1. _____
(перечислить все необходимые сведенья)

2. _____

Идентификационные данные пользователя, информацию о создании ЭП или ключа ЭП которого необходимо предоставить:

_____

Время и дата формирования ЭП или ключа ЭП, в отношении которых возникла конфликтная ситуация:

_____

Сертификат Пользователя СЭП в электронной форме, с использованием которого создана электронная подпись, в отношении которой производится разбор конфликтной ситуации прилагается на CD(DVD) (или flash-носителе).

Приглашаем принять участие в рабочем совещании разрешительной комиссии в ЧЧ:ММ ДД.ММ.ГГГГ по адресу: г. Москва, ул._____, д.__

Председатель разрешительной комиссии: _____
(ФИО, email, номер мобильного телефона)

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

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

«___»_____20__ г.

М.П.

Приложение № 12 к Регламенту Сервиса электронной подписи
ООО «КРИПТО-ПРО»
(Форма письменного согласия субъекта персональных данных)

Согласие на обработку персональных данных

Я,_____,
(*Ф.И.О. полностью*)

проживающий по адресу:_____,
паспорт №_____ серия _____, выданный (кем и когда)_____
_____,
настоящим даю свое согласие
_____
(указывается наименование Уполномоченной организации, ИНН, юридический адрес)

на обработку и передачу ООО «КРИПТО-ПРО» (ИНН 7717107991, 105318, г.Москва, ул.Ибрагимова, д. 31, офис 30Б) следующих моих персональных данных, заносимых в сертификаты ключей проверки электронной подписи, владельцем которых я являюсь:

- фамилия, имя, отчество;
- СНИЛС;
- ИНН;
- адрес места регистрации (страна, субъект РФ, населенный пункт, улица, номер дома, корпуса, строения, квартиры);
- адрес электронной почты;
- номер телефона.

Настоящим я подтверждаю, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным, не являются тайной частной жизни, личной и (или) семейной тайной.

Предоставляемые мною персональные данные могут использоваться только в целях обработки персональных данных связанных с надлежащим и своевременным получением услуг Сервиса электронной подписи.

_____ и
(указывается наименование Уполномоченной организации, ИНН, юридический адрес)

ООО «КРИПТО-ПРО» имеют право на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения вышеуказанных целей обработки персональных данных, включая (без ограничения) сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение, предоставление, доступ, распространение, трансграничную передачу, а также осуществление любых иных действий с моими персональными данными, предусмотренных законодательством Российской Федерации.

Я подтверждаю, что, подписывая настоящее согласие, действую своей волей и в своих интересах.

Настоящее согласие на обработку и передачу персональных данных предоставлено мною с «__» _____ 20__ г. на _____ (*указывается срок, на который предоставлено согласие*), но не менее срока получения услуг Сервиса электронной подписи.

Настоящее заявление (согласие) на передачу персональных данных может быть отозвано мной в письменной форме.

Дата: «___» _____ 20__г. Подпись_____ /_____/