Утвержден
Приказом ООО «КРИПТО-ПРО» № 24/02-01
от «15» февраля 2024 г.

РЕГЛАМЕНТ
ООО «КРИПТО-ПРО»
по предоставлению услуг Сервиса электронной подписи с возможностью выпуска сертификатов усиленной электронной подписи (Схема обслуживания: операторская)

(Регламент Сервиса ЭП)

Редакция № 2

г. Москва
2024

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: 105037, г. Москва, вн. тер. г. муниципальный округ Измайлово, Измайловский проезд, д. 10, к. 2, помещ. 4/1
Адрес для направления корреспонденции: 127018, г. Москва, ул. Сущевский Вал, д. 18
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 от 6 апреля 2011 года №63-ФЗ «Об электронной подписи» (далее – Федеральный закон «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.

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

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

Ключ электронной подписи 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 – ключ аутентификации в мобильном приложении СЭП на устройствах пользователей; 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, выдаваемый 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.

Мобильное приложение СЭП – компонент СЭП, устанавливаемый на мобильном устройстве Пользователей СЭП.

Обращение - сообщение по вопросам, связанным с осуществлением доступа к СЭП, Уполномоченной организации или Оператора Сервиса электронной подписи, отправленное через Портал технической поддержки в адрес Исполнителя, содержащее в себе реквизиты Договора, заключенного с Исполнителем на оказание услуг СЭП

Оператор Стороннего центра идентификации (Оператор СЦИ) – Оператор СЭП, зарегистрированный в Стороннем центре идентификации Уполномоченной организации, действующий от имени Уполномоченной организации по обеспечению создания Пользователем СЭП 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 Пользователем СЭП 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/или являющееся владельцем сертификата ключа проверки электронной подписи либо физическое лицо, действующее от имени владельца сертификата ключа проверки электронной подписи, если владелец сертификата ключа проверки 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.

Портал технической поддержки (Портал) – информационный ресурс Исполнителя, размещенный по адресу в сети Интернет: https://support.cryptopro.ru, предназначенный для приёма и обработки обращений в целях проведения консультаций по вопросам, связанным с осуществлением доступа к СЭП.

Прикладной интерфейс СЭП (API) – интерфейс подключения Информационных систем Уполномоченной организации к техническим средствам Исполнителя по линиям связи для получения доступа к функциям электронной подписи, управления сертификатами ключей проверки электронной подписи, реализованный в соответствии с руководством разработчика на программное обеспечение СЭП и защищенный с использованием средств криптографической защиты информации, совместимых со средствами Исполнителя.

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, имеющем право доступа к СЭП, и используемая при создании Сертификата Пользователя СЭП (содержится в сведениях о владельце этого сертификата (в поле Subject)).

Сервис электронной подписи (СЭП) – комплекс организационных, технических и программных средств, обеспечивающих для Пользователей СЭП удаленную реализацию функций централизованного создания и хранения ключей электронной подписи, создания и проверки усиленной электронной подписи электронных документов, выпуска и управления сертификатами ключей проверки электронной подписи, аутентификации владельцев

сертификатов ключей проверки электронной подписи при осуществлении доступа к СЭП и выполнении операций с использованием принадлежащих им ключей электронной подписи.

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 пользователя СЭП (Сертификат ключа проверки электронной подписи Пользователя СЭП) – сертификат ключа проверки электронной подписи, выданный Исполнителем посредством СЭП или зарегистрированный в СЭП Пользователем 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) – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

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 по стандартным протоколам и используемая Уполномоченной организацией для управления доступом Пользователей СЭП к Сервису электронной подписи.

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 применения российских криптографических алгоритмов.

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 мобильного приложения СЭП.

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 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/reglamentoperdssallca.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 осуществляет свою деятельность в соответствии с лицензией 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). С копией указанной лицензии можно ознакомиться по следующему адресу в сети Интернет - http://www.cryptopro.ru/about/licenses.

4.2. Исполнитель вправе запросить, а Уполномоченная организация обязана предоставить Исполнителю следующие документы:

- 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 № 6 к Регламенту.

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

5.1.10. 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 настоящего Регламента.

5.1.11. Предоставить по запросу Уполномоченной организации на уточнение и согласование перечень параметров настройки функционирования СЭП, аутентификации Операторов СЭП и Пользователей СЭП к СЭП по форме, установленной в Приложении № 7 к Регламенту.

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

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

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

5.1.15. Предоставить Уполномоченной организации необходимые права для:

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

5.1.15.2. регистрации Пользователей в СЭП;

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

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

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

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

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

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

5.1.18. По заявлению Уполномоченной организации в соответствии с формой, приведенной в Приложении № 12 к Регламенту, и согласно положениям настоящего Регламента предоставить сведения, а также принять участие в работе разрешительной комиссии для разбора конфликтной ситуации, связанной с применением электронной подписи, созданной с использованием СЭП.

5.1.19. 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.

5.1.20. Проводить консультации представителям Уполномоченной организации, в том числе Операторам СЭП, по вопросам, связанным с осуществлением доступа к СЭП с использованием Мобильного приложения СЭП, Веб- и Прикладного интерфейса, предоставляемых Исполнителем в соответствии с настоящим Регламентом. Консультации предоставляются в рабочие дни, в рамках обработки обращений, оформленных представителями Уполномоченной организации, в том числе Операторами СЭП, через Портал.

5.1.21. Принять меры к восстановлению доступности СЭП при получении обращения от Уполномоченной организации.

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 настоящего 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.

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, установленной в Приложении № 7 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. 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.

5.2.13.6. 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.

5.2.13.7. 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.

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

5.2.13.9. 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.

5.2.13.10 Незамедлительно уведомить Исполнителя посредством оформления обращения на Портале технической поддержки о недоступности СЭП и оказать специалистам Исполнителя содействие в установлении причин нарушения доступности СЭП, в т.ч. предоставить детальное описание возникших проблем при работе с СЭП и дополнительную информацию при получении запроса на уточнение исходных данных от специалистов Исполнителя. При получении ответа от специалистов Исполнителя о функционировании СЭП в штатном режиме принять меры для выявления и устранения проблем в функционировании подключенной к СЭП Информационной системы Уполномоченной организации. При регистрации представителя Уполномоченной организации для оформления обращений на Портале технической поддержки должны быть указаны реквизиты Уполномоченной организации.

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 непредоставления 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, установленной в Приложении № 7 к Регламенту.

5.3.7. Отказать в подключении Стороннего центра идентификации Уполномоченной организации в случае ненадлежащего оформления заявления на подключение Стороннего центра идентификации, форма которого установлена в Приложении № 9 к Регламенту.

5.3.8. Отказать в подключении SMS-шлюза Уполномоченной организации в случае ненадлежащего оформления заявления на подключение SMS-шлюза, форма которого установлена в Приложении № 8 к Регламенту.

5.3.9. Отказать в регистрации Оператора СЦИ до получения надлежащим образом оформленного заявления на подключение Стороннего центра идентификации Уполномоченной организации (форма которого установлена в Приложении № 9 к Регламенту) или в случае ненадлежащего оформления заявления на регистрацию Оператора СЦИ, форма которого установлена в Приложении № 10 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 аутентификация 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, установленной в Приложении № 7 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, установленной в Приложении № 1 к Регламенту, и в порядке, установленном п.8.1 настоящего 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, установленной в Приложении № 10 к Регламенту, и в порядке, установленном настоящим Регламентом.

5.4.6. Подключать к СЭП Удостоверяющие центры в соответствии с настоящим Регламентом для автоматической отправки сформированных запросов на создание и управление Сертификатами Пользователей СЭП, получения и установки в СЭП созданных Сертификатов СЭП. Для подключения к СЭП Удостоверяющего центра должна быть техническая возможность и совместимость программных средств СЭП со средствами Удостоверяющего центра. Решение о возможности подключения СЭП к Удостоверяющему центру принимает Исполнитель.

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 или Мобильного приложения СЭП с отправкой их в подключенный Удостоверяющий центр. Предоставленные Уполномоченной организацией права Пользователей СЭП определяются параметрами функционирования СЭП в соответствии с Приложением № 7 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. Запрашивать консультации у Исполнителя по вопросам, связанным с осуществлением доступа к СЭП с использованием Веб- и Прикладного интерфейса, предоставляемых Исполнителем в соответствии с настоящим Регламентом, путем создания обращения через Портал. Обращение должно содержать реквизиты Договора, заключенного Уполномоченной организацией с Исполнителем на оказание услуг СЭП.

5.4.13. Оператор СЭП имеет право:

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

5.4.13.2. Формировать запросы на создание Сертификатов Пользователей СЭП.

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

5.4.13.4. Запрашивать консультации у Исполнителя по вопросам, связанным с осуществлением доступа к СЭП с использованием Веб- и Прикладного интерфейса, предоставляемых Исполнителем в соответствии с настоящим Регламентом, путем создания обращения через Портал. Обращение должно содержать реквизиты Договора, заключенного Уполномоченной организацией с Исполнителем на оказание услуг СЭП.

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 произошло 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. Присоединяясь к настоящему Регламенту, Уполномоченная организация в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» поручает Исполнителю совершать с персональными данными, содержащимися в документах, представленных Уполномоченной организацией Исполнителю для присоединения к настоящему Регламенту, а также в документах, которые будут представлены Уполномоченной организацией Исполнителю в соответствии с Регламентом, следующие действия (с использованием и без использования средств автоматизации): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача, обезличивание, блокирование, удаление, уничтожение персональных данных (далее – «обработка»),- в целях присоединения Уполномоченной организации к Регламенту и предоставления услуг, связанных с СЭП, в целях исполнения Регламента, реализации вытекающих из Регламента прав и обязанностей, а также в целях осуществления Удостоверяющим центром функций по созданию, выпуску, выдаче и управлению сертификатами ключей проверки электронной подписи, подтверждению подлинности электронной подписи электронных документов.

7.2. Уполномоченная организация поручает Исполнителю осуществлять обработку персональных данных субъектов персональных данных, содержащихся в документах, представленных Уполномоченной организацией, с соблюдением принципов и правил обработки персональных данных, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», и обеспечением безопасности персональных данных при их обработке, на безвозмездной основе.

7.3. Уполномоченная организация гарантирует и подтверждает, что ею получены письменные согласия субъектов персональных данных, чьи персональные данные содержатся в представленных Уполномоченной организацией Исполнителю документах, на обработку Исполнителем этих персональных данных по поручению Уполномоченной организации в указанных выше целях, а также гарантирует, что документы, содержащие персональные данные субъектов персональных данных, будут представляться Уполномоченной организацией Исполнителю в соответствии с Регламентом с согласия субъектов персональных данных, чьи персональные данные содержатся в таких документах. Письменное согласие Оператора СЭП на обработку его персональных данных Исполнителем оформляется в форме Заявления на регистрацию Оператора СЭП (Приложение №1 к настоящему Регламенту). Письменное согласие Пользователя на обработку его персональных данных Исполнителем оформляется с соблюдением требований, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (рекомендуемая форма установлена Приложением №13 к Регламенту). Уполномоченная организация несет все неблагоприятные последствия, связанные с неполучением Уполномоченной организацией таких согласий или их несоответствия Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных».

7.4. Уполномоченная организация гарантирует и подтверждает, что ею получены письменные согласия субъектов персональных данных, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых они являются, относятся к персональным данным, предоставление которых разрешено субъектом персональных данных в составе сертификата ключей проверки электронной подписи.

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

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

8.1. Взаимодействие Оператора СЭП с СЭП

8.1.1. Подключение Оператора СЭП к СЭП

Подключение Оператора СЭП к СЭП осуществляется на основании заявления на регистрацию Оператора СЭП и доверенности Оператора СЭП. Форма заявления на регистрацию Оператора СЭП приведена в Приложении № 1 к Регламенту, форма доверенности Оператора СЭП приведена в Приложении № 2 к Регламенту.

Предоставление заявительных документов для регистрации Оператора СЭП может быть осуществлено:

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

По согласованию с Исполнителем заявительные документы могут предоставляться в форме электронного документа, подписанного квалифицированными электронными подписями тех лиц, которые должны подписать данные документы.

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

После успешной регистрации Оператор СЭП должен получить сертификат ключа проверки электронной подписи в соответствии с пунктом 8.1.2 настоящего Регламента. С использованием указанного сертификата будет производиться подключение Оператора СЭП к СЭП.

8.1.2. Получение Оператором СЭП сертификата ключа проверки электронной подписи для подключения к СЭП

Для подключения Оператора СЭП к СЭП используется неквалифицированный сертификат ключа проверки электронной подписи, который создается Исполнителем.

Получение сертификата ключа проверки электронной подписи Оператора СЭП осуществляется при личном прибытии Оператора СЭП (либо иного полномочного представителя Уполномоченной организации) в офис Исполнителя по предварительному согласованию с Администратором СЭП, и производится в течение рабочего дня прибытия Оператора СЭП.

Оператор подает заявление на создание сертификата ключа проверки электронной подписи по форме, установленной в Приложении № 4 к Регламенту, и предоставляет носитель ключа электронной подписи, поддерживаемый средством электронной подписи.

На основании предоставленного заявления Администратор СЭП осуществляет формирование ключей электронной подписи и проверки электронной подписи, запись ключа электронной подписи на предоставленный носитель, создание сертификата ключа проверки электронной подписи, запись сертификата ключа проверки электронной подписи на предоставленный ключевой носитель и распечатывает по форме Приложения №14 к Регламенту сведения из сертификата ключа проверки электронной подписи.

Сведения из сертификата ключа проверки электронной подписи Оператора СЭП визируются Оператором СЭП (либо иным полномочным представителем Уполномоченной организации) и предоставляются Администратору СЭП.

По согласованию с Исполнителем заявительные документы могут предоставляться в форме электронного документа, подписанного квалифицированными электронными подписями тех лиц, которые должны подписать данные документы.

Также по согласованию с Исполнителем и при наличии у Оператора СЭП квалифицированного сертификата ключа проверки электронной подписи, Оператор СЭП может осуществить формирование пары ключей (ключей электронной подписи и проверки электронной подписи) и формирование запроса на сертификат ключа проверки электронной подписи в файл формата PKCS#10 в кодировке Base64. Для формирования запроса на сертификат Оператор СЭП может использовать html-файл, получаемый от Администратора СЭП, или иное специальное ПО, совместимое со средствами электронной подписи и средствами удостоверяющего центра. Созданный файл с запросом на сертификат формата PKCS#10 подписывается квалифицированной электронной подписью Оператора СЭП.

Администратор СЭП на основании указанного файла, а также необходимых заявительных документов, создает сертификат ключа проверки электронной подписи Оператора СЭП и направляет Оператору СЭП по электронной почте форму сведений из сертификата ключа проверки электронной подписи согласно Приложению №14 к Регламенту. Оператор СЭП должен подписать своей квалифицированной электронной подписью сведения из сертификата и направить их Администратору СЭП.

После выпуска Оператору СЭП сертификата Администратором СЭП предоставляются Оператору СЭП параметры настройки функционирования СЭП, включающие URL-адреса подключения к СЭП Оператора СЭП и Пользователей СЭП, Информационных систем и прочие необходимые для подключения данные. Информация может быть отправлена на адрес электронной почты, указанный в заявлении на регистрацию Оператора СЭП, и зашифрована с использованием ключа проверки электронной подписи, содержащимся созданном сертификате оператора Сертификате СЭП.

8.1.3. Плановая смена Оператором СЭП сертификата ключа проверки электронной подписи для подключения к СЭП

Создание нового сертификата ключа проверки электронной подписи Оператора СЭП осуществляется по заявлению на создание сертификата не ранее 30-ти календарных дней и не позднее 5-ти календарных дней до окончания срока действия ключа электронной подписи Оператора СЭП.

Заявления, оформленные согласно данному разделу настоящего Регламента, поступившие Исполнителю ранее или позднее установленного срока, рассмотрению не подлежат.

Оператор СЭП осуществляет формирование пары ключей (ключей электронной подписи и проверки электронной подписи) и формирование запроса на сертификат ключа проверки электронной подписи в файл формата PKCS#10 в кодировке Base64.

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

Созданный файл с запросом на сертификат формата PKCS#10 подписывается электронной подписью Оператора СЭП на действующем ключе подписи Оператора СЭП. Указанный документ с электронной подписью Оператора СЭП признается заявлением на создание сертификата ключа проверки электронной подписи. Данное заявление направляется Оператором СЭП Администратору СЭП.

Администратор СЭП на основании поступившего заявления на создание сертификата ключа проверки электронной подписи создает сертификат ключа проверки электронной подписи Оператора СЭП и направляет Оператору СЭП по электронной почте форму сведений из сертификата ключа проверки электронной подписи согласно Приложению №14 к Регламенту.

Оператор СЭП должен подписать своей электронной подписью сведения из сертификата и направить их Администратору СЭП.

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

После подтверждения получения Исполнителем завизированных Оператором СЭП сведений из сертификата ключа проверки электронной подписи и регистрации Администратором СЭП полученного сертификата в СЭП, Оператор СЭП может использовать для выполнения возложенных на него обязанностей новый сертификат ключа проверки электронной подписи и соответствующий ему ключ электронной подписи.

8.1.4. Внеплановая смена Оператором СЭП сертификата ключа проверки электронной подписи для подключения к СЭП

Внеплановая смена сертификата ключа проверки электронной подписи Оператора СЭП осуществляется Оператором СЭП в следующих случаях:

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

Формирование ключей и создание сертификата ключа проверки электронной подписи Оператора СЭП осуществляется в соответствии с разделом 8.1.2 настоящего Регламента.

8.1.5. 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 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.

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

Подача заявления на прекращение доступа к СЭП по форме Приложения № 5 к Регламенту осуществляется Оператором СЭП посредством почтовой или курьерской связи.

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 настоящего Регламента номеру телефона.

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.

8.1.5.2. 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 № 5 к 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.

8.1.5.3. Прекращение доступа Оператора СЭП к СЭП по прекращению действия Сертификата Оператора СЭП или истечению срока действия соответствующего ключа электронной подписи.

В случае прекращения 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 разделом 8.2. настоящего Регламента.

8.1.5.4. 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 или Уполномоченной организации 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.

8.2. Выпуск неквалифицированных сертификатов ключей проверки электронной подписи Пользователям СЭП

Оператор СЭП может обеспечить выпуск неквалифицированных сертификатов ключей проверки электронной подписи Пользователям СЭП с использованием средства удостоверяющего центра, развернутого у Исполнителя.

Регистрация Пользователей СЭП в удостоверяющем центре, обеспечение создания для них сертификатов ключей проверки электронной подписи и обеспечение управления сертификатами ключей проверки электронной подписи, производится Оператором СЭП и осуществляется в соответствии с порядком, который устанавливается Уполномоченной организацией.

Исполнитель выполняет действия по созданию сертификатов ключей проверки электронной подписи, прекращению действия сертификатов ключей проверки электронной подписи, приостановлению и возобновлению действий сертификатов ключей проверки электронной подписи в соответствии с настройками параметров функционирования СЭП, на основании заявок в электронной форме внутреннего формата СЭП, направляемых Оператором СЭП и (или) Пользователями с использованием Мобильного приложения СЭП, Веб- или Прикладного интерфейса СЭП, предоставляемого Исполнителем. Выполнение указанных действий осуществляется Исполнителем при соответствии параметров аутентификации заявителя регистрационным данным:

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

Регистрация всех операций, выполняемых Операторами и Пользователями СЭП, осуществляется средствами СЭП. При согласии Исполнителя 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 Мобильного приложения СЭП, Веб- или Прикладного интерфейса, предоставляемого СЭП, на основании аутентификационной информации, переданной Уполномоченной организацией при регистрации и подключении Пользователя в СЭП или полученной от Стороннего центра идентификации Уполномоченной организации.

Функции создания электронной подписи посредством СЭП доступны владельцам действующих сертификатов ключей проверки электронной подписи.

В случае хранения ключа ЭП в СЭП владелец сертификата ключа проверки электронной подписи 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 или адрес электронной почты, 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.

8.3. Выпуск квалифицированных сертификатов ключей проверки электронной подписи Пользователям СЭП

Оператор СЭП может обеспечить выпуск квалифицированных сертификатов ключей проверки электронной подписи Пользователям СЭП в аккредитованном удостоверяющем центре, с которым у Исполнителя заключен соответствующий договор на обслуживание.

Регистрация Пользователей СЭП в аккредитованном удостоверяющем центре, обеспечение создания для них квалифицированных сертификатов ключей проверки электронной подписи и обеспечение управления сертификатами ключей проверки электронной подписи, производится Оператором СЭП и осуществляется в соответствии с Порядком реализации функций аккредитованного удостоверяющего центра. Указанный Порядок размещается на официальном сайте аккредитованного удостоверяющего центра.

Действия по выпуску квалифицированных сертификатов ключей проверки электронной подписи, прекращению действия квалифицированных сертификатов ключей проверки электронной подписи осуществляется в соответствии с настройками параметров функционирования СЭП на основании заявок в электронной форме внутреннего формата СЭП, направляемых Оператором СЭП и (или) Пользователями СЭП с использованием Мобильного приложения СЭП, Веб- или Прикладного интерфейса СЭП, предоставляемого Исполнителем. Выполнение указанных действий осуществляется Исполнителем при соответствии параметров аутентификации заявителя регистрационным данным:

- Подтвержден уникальный идентификатор Центра идентификации СЭП или Стороннего центра идентификации Уполномоченной организации, в котором зарегистрирован Оператор СЭП и (или) Пользователь СЭП;
- Сертификат ключа проверки электронной подписи Оператора СЭП на момент получения заявки Исполнителем действителен или идентификатор Оператора СЭП получен от Стороннего центра идентификации Уполномоченной организации.
- Аутентификация Пользователя СЭП подтверждена с использованием ключа аутентификации в мобильном приложении СЭП или СКЗИ «КриптоПро CSP» на рабочем месте Пользователя СЭП 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 Операторами СЭП и Пользователями СЭП, осуществляется средствами СЭП. При согласии Исполнителя 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 Мобильного приложения СЭП, Веб- или Прикладного интерфейса, предоставляемого Исполнителем, на основании аутентификационной информации, переданной Уполномоченной организацией при регистрации и подключении Пользователя СЭП в СЭП или полученной от Стороннего центра идентификации Уполномоченной организации.

Функции создания электронной подписи посредством СЭП доступны владельцам действующих сертификатов ключей проверки электронной подписи.

8.4. Подключение Информационной системы Уполномоченной организации к СЭП

Исполнитель предоставляет Уполномоченной организации Прикладной интерфейс подключения к СЭП. Защита передаваемых от Информационной системы к СЭП данных осуществляется в соответствии с требованиями Уполномоченной организации с использованием СКЗИ, совместимых со средствами 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, установленной в Приложении № 7 к Регламенту.

8.5. Подключение SMS-шлюза Уполномоченной организации к СЭП

Подключение SMS-шлюза Уполномоченной организации к СЭП осуществляется по заявлению Уполномоченной организации по форме, установленной в Приложении № 8 к Регламенту.

Настройка параметров СЭП для подключения SMS-шлюза Уполномоченной организации осуществляется в течение 5 (пяти) рабочих дней с даты получения подписанного заявления по форме, установленной в Приложении № 8 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 Службы проверки сертификатов и электронной подписи «КриптоПро SVS» к СЭП

Подключение Службы проверки сертификатов и электронной подписи «КриптоПро SVS» осуществляется по заявлению Уполномоченной организации по форме, установленной в Приложении № 15 к Регламенту.

Настройка сервиса проверки сертификатов осуществляется в течении 5 (пяти) рабочих дней с даты получения подписанного заявления по форме, установленной в Приложении № 15 к Регламенту.

В случае необходимости изменения параметров настройки функционирования службы проверки Уполномоченная организация после предварительного согласования в рабочем порядке направляет Исполнителю подписанный исправленный вариант параметров настройки СЭП по форме, установленной в Приложении № 15 к Регламенту.

При необходимости проверки сертификатов, выданных Удостоверяющим центром, точки распространения списков отзыва которого не доступны из сети Интернет, Уполномоченная организация предоставляет Исполнителю CRL со сроком действия не менее 3 месяцев и принимает на себя риски, связанные с возможностью некорректной проверки недействительного сертификата на основании полученного Исполнителем CRL.

8.7. Подключение стороннего центра идентификации Уполномоченной организации к СЭП

Подключение СЦИ к СЭП осуществляется по заявлению Уполномоченной организации по форме, установленной в Приложении № 9 к Регламенту. Вместе с заявлением на носителе информации или по электронной почте 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, установленной в Приложении № 9 к Регламенту.

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

Регистрация Оператора СЦИ в СЭП выполняется после получения заявления по форме, установленной в Приложении № 10 к Регламенту.

8.8. Подключение стороннего Удостоверяющего центра к СЭП

Подключение стороннего 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 по заявлению Уполномоченной организации по форме, установленной в Приложении № 11 к Регламенту. Вместе с заявлением на носителе информации или по электронной почте 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» версии 2.0 и выше, 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, установленной в Приложении № 11 к Регламенту.

Настройку средств УЦ для подключения к СЭП обеспечивает Уполномоченная организация.

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

8.9. 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 в соответствии с параметрами настройки функционирования СЭП, предоставленных Уполномоченной организацией и согласованных с Исполнителем по форме, установленной в Приложении №7 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. При согласии Исполнителя 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 СЭП и установлен в СЭП.
4. Список отозванных сертификатов УЦ -издателя сертификата Пользователя СЭП 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 или адрес электронной почты, 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 сроком действия Договора.

8.10. 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 № 7 к Регламенту.

8.11. Участие Исполнителя в экспертизе электронной подписи

По запросу Уполномоченной организации Исполнитель может принять участие в проведении экспертных работ по разбору 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 № 12 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.

На основании потупившего заявления Исполнитель оценивает объём работ, связанных с предоставлением запрашиваемых данных. Исполнитель вправе установить вознаграждение за поиск и предоставление данных, необходимых для работы разрешительной комиссии.

В срок не более 10 (десяти) рабочих дней с даты получения заявления Исполнитель предоставляет Уполномоченной организации отчет, в котором указывает размер вознаграждения за предоставление запрашиваемых данных (при принятии такого решения Исполнителем), запрошенные данные (если Исполнитель не видит необходимости в запросе вознаграждения за предоставление данных), условия своего участия в разрешительной комиссии.

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

В случае применения в СЭП неквалифицированных сертификатов ключей проверки электронной подписи, созданных удостоверяющим центром Исполнителя, Исполнитель может осуществить по обращению Уполномоченной организации подтверждение подлинности электронной подписи в электронном документе, подписанном указанным сертификатом.

Проверка электронной подписи, созданной средствами СЭП на неквалифицированном сертификате ключа проверки электронной подписи, выданном удостоверяющим центром Исполнителя, осуществляется с использованием СЭП и (или) локальными средствами электронной подписи, совместимыми со средствами СЭП.

По запросу Уполномоченной организации, удостоверяющий центр Исполнителя осуществляет проведение экспертных работ по подтверждению электронной подписи в электронном документе, созданной с использованием Сервиса электронной подписи на неквалифицированном сертификате ключа проверки электронной подписи, выданном удостоверяющим центром Исполнителя. В отношении электронных документов, подписанных электронной подписью с использованием сертификатов ключей проверки электронной подписи, созданных удостоверяющими центрами отличными от удостоверяющего центра Исполнителя, работы по подтверждению подлинности электронной подписи Исполнитель не производит.

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

В данном случае для подтверждения подлинности ЭП в электронных документах Уполномоченная организация подает заявление Исполнителю по форме, приведенной в Приложении №12.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;

- время и дата, на момент наступления которых требуется установить подлинность ЭП.

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

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

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

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

Заключение содержит:

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

Отчет по выполненной проверке содержит:

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

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

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

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

9. Структура запросов на создание сертификатов ключей проверки электронной подписи, форма 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.

9.2. Форма квалифицированного сертификата ключа проверки электронной подписи и сроки действия ключевых документов, связанных с квалифицированными сертификатами

9.2.1. Форма квалифицированного сертификата ключа проверки электронной подписи соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи». Квалифицированный сертификат ключа проверки электронной подписи создается аккредитованным удостоверяющим центром в соответствии с Порядком реализации функций аккредитованного удостоверяющего центра.

9.2.2. Сроки действия ключей подписи и соответствующих им квалифицированным сертификатам ключей проверки электронной подписи устанавливаются аккредитованным удостоверяющим центром в соответствии с Порядком реализации функций аккредитованного удостоверяющего центра.

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

9.3. Форма неквалифицированного сертификата ключа проверки электронной подписи и сроки действия ключевых документов, связанных с неквалифицированными сертификатами, создаваемыми удостоверяющим центром Исполнителя

9.3.1. Форма неквалифицированного сертификата ключа проверки электронной подписи удостоверяющего центра Исполнителя

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
SerialNumber	Серийный номер	Уникальный серийный номер сертификата
SignatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
ValidityPeriod	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = УЦ КРИПТО-ПРО Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
PublicKey	Открытый ключ	Ключ проверки электронной подписи (алгоритм ГОСТ Р 34.10-2012)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий;

		Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа электронной подписи Удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SybjectType (Тип владельца сертификата) =ЦС PathLengthConstraint (Ограничение на длину пути –ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата Удостоверяющего центра

9.3.2. Форма неквалифицированного сертификата ключа проверки электронной подписи Пользователя СЭП

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийныйномер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритмподписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО Organization(Организация) = ООО КРИПТО-ПРО Locality(Город)= Москва Country(Страна)= RU Email(Электронная почта) = cpca@cryptopro.ru
ValidityPeriod	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата и Оператором Удостоверяющего центра. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
PublicKey	Открытый ключ	Ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Электронная подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Набор областей использования ключей и сертификатов за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Application Policy	Политика применения	Набор областей использования ключей и сертификатов за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора ключа электронной подписи Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов

Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа проверки электронной подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

9.3.3. Форма списка отозванных сертификатов (CRL) удостоверяющего центра Исполнителя

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ КРИПТО-ПРО – псевдоним Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (ResonCode) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата ключа проверки электронной подписи (корневого сертификата) Удостоверяющего Центра

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

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

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

9.3.5. Срок действия ключа электронной подписи Оператора СЭП, связанного с неквалифицированным сертификатом, созданным удостоверяющим центром Исполнителя, составляет 1 (один) год.

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

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

9.3.6. Срок действия ключа электронной подписи Пользователя СЭП, связанного с неквалифицированным сертификатом, созданным удостоверяющим центром Исполнителя, составляет 1 (один) год.

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

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

9.4. Использование ключей электронной подписи после окончания срока их 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 в соответствии с порядком, установленным удостоверяющим центром, создавшим этот сертификат.

10.2. Конфиденциальность информации

10.2.1. Типы конфиденциальной информации

10.2.1.1. Ключ электронной подписи, соответствующий сертификату Пользователя СЭП, является конфиденциальной информацией лица, зарегистрированного в 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. 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 хранения 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 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.

10.5. Ограничения, связанные с использованием СЭП

10.5.1. В случае, если средство электронной подписи, с использованием которого обеспечивается эксплуатация СЭП, не будет иметь подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», то с использованием Сервиса электронной подписи может быть сформирована только усиленная неквалифицированная электронная подпись.

11. Список приложений

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

11.2. Приложение № 2. Форма доверенности Оператора СЭП.

11.3. Приложение № 3. Форма доверенности на предоставление заявительных документов Оператора СЭП.

11.4. Приложение № 4. Форма заявления на создание сертификата ключа проверки электронной подписи Оператора СЭП.

11.5. Приложение № 5. Форма заявления на прекращение доступа Оператора СЭП к СЭП.

11.6. Приложение № 6. Функции Сервиса электронной подписи.

11.7. Приложение № 7 Форма перечня параметров функционирования СЭП для настройки доступа Операторов и Пользователей СЭП.

11.8. Приложение № 8. Форма заявления на подключение SMS-шлюза.

11.9. Приложение № 9. Форма заявления на подключение Стороннего центра идентификации.

11.10. Приложение № 10. Форма заявления на регистрацию Оператора СЦИ.

11.11. Приложение № 11. Форма заявления на подключение Удостоверяющего центра.

11.12. Приложение № 12. Форма запроса на предоставление информации для разбора конфликтной ситуации. Форма заявления на подтверждение подлинности ЭП.

11.13. Приложение № 13. Рекомендуемая форма письменного согласия субъекта персональных данных.

11.14. Приложение № 14. Форма сведений из сертификата ключа проверки электронной подписи.

11.15. Приложение № 15. Форма заявления на подключение дополнительного сервиса проверки электронной подписи к Сервису электронной подписи ООО «КРИПТО-ПРО».

Приложение №1 к Регламенту Сервиса ЭП
(Форма заявления на регистрацию Оператора СЭП)

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

по Договору №_____ от ___.___._____ г.

_____
(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 ЭП, по:

1. _____;*
2. _____;*
3. _____.*

* - Указать одну или несколько необходимых позиций из следующих:

- обеспечить выпуск неквалифицированных сертификатов, создаваемых ООО «КРИПТО-ПРО»;
- обеспечить выпуск квалифицированных сертификатов в аккредитованном УЦ, заключившем Договор с ООО «КРИПТО-ПРО»;
- подключить к экземпляру Сервиса электронной подписи, функционирование которого должно быть настроено согласно Приложения 7 к Регламенту.

Настоящим _____
(фамилия, имя, отчество)

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

соглашается с обработкой своих персональных данных, содержащихся в настоящем заявлении. ООО «КРИПТО-ПРО» имеет право обрабатывать мои персональные данные следующими способами: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных. Настоящее согласие на обработку своих персональных данных ООО «КРИПТО-ПРО» дано на срок регистрации в Сервисе электронной подписи ООО «КРИПТО-ПРО» и в течение 3(трех) лет после прекращения регистрации в Сервисе электронной подписи ООО «КРИПТО-ПРО».

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

В целях надлежащего и своевременного оказания ООО «КРИПТО-ПРО» услуг

_____

(фамилия, имя, отчество)

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)

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

Подпись уполномоченного представителя организации _____ /_____/

«____» _____ 20____ г.

_____ _____ /_____/

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

«____» _____ 20____

М.П.

Приложение №2 к Регламенту Сервиса ЭП
(Форма доверенности 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)

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

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

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

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

«____» _____ 20____
М.П.

Приложение №3 к Регламенту Сервиса ЭП
(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 ЭП для регистрации своего полномочного представителя - Оператора СЭП

_____
(фамилия, имя, отчество Оператора СЭП)

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 №4 к Регламенту Сервиса ЭП
(Форма заявления на создание сертификата
ключа проверки электронной подписи Оператора СЭП)

Заявление на создание сертификата ключа проверки электронной подписи Оператора СЭП

по Договору №_____ от ___.___._____ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит сформировать ключи электронной подписи, записать сформированный ключ электронной подписи на предоставленный ключевой носитель и создать сертификат ключа проверки электронной подписи своего уполномоченного представителя – Оператора СЭП:

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
OrganizationUnit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Country (C)	RU	

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

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

«____» _____ 20____.
М.П.

Приложение № 5 к Регламенту Сервиса ЭП
(Форма заявления на прекращение доступа Оператора СЭП к СЭП)

Заявление на прекращение доступа Оператора СЭП к СЭП

по Договору №_____ от ___.___._____ г.

_____
(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: _____
(фамилия, имя, отчество)

и прекратить действие сертификата ключа проверки электронной подписи, содержащего следующие идентификационные данные:

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

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 №6 к Регламенту Сервиса ЭП
(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» версии 2.0 и выше.

2. Поддерживаемые форматы и стандарты

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

Поддерживаемые форматы криптографических сообщений:

1. Электронная подпись ГОСТ 34.10 – 2012;
2. Усовершенствованная подпись в соответствии с ETSI TS 101 733 "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)", рекомендациями RFC 5652, "Cryptographic Message Syntax" (CAdES-BES, 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 руководством разработчика программного обеспечения СЭП.

Аутентификация пользователей осуществляется с использованием штатного Центра идентификации или по протоколу WS-Federation или OpenID Connect 1.0 с использованием

Стороннего центра идентификации Уполномоченной организации, подключаемого к Сервису электронной подписи в соответствии с документацией напрограммное обеспечение СЭП.

Руководства доступны по адресу https://www.cryptopro.ru/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 СЭП

СЭП позволяет информировать Пользователей СЭП посредством отправки по электронной почте или с использованием SMS-шлюза информационных сообщений, 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 № 7 к Регламенту Сервиса ЭП
(Форма перечня параметров функционирования СЭП
для настройки доступа Операторов и Пользователей СЭП)

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

по Договору №_____ от ___.___._____ г.

_____
(полное наименование Уполномоченной организации, включая организационно-правовую форму)
в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____,
подтверждает подключение к Сервису электронной подписи ООО «КРИПТО-ПРО» в соответствии с указанными в таблице ниже значениями параметров функционирования (целевые значения параметров необходимо отмечать символом «+»; **первоначально отмечены символом «+» значения по умолчанию**) экземпляра СЭП:

№ п/п	Параметр СЭП	Настраиваемое значение параметра СЭП	
1.	Наименование экземпляра СЭП[1]		
2.	Использование веб-интерфейса СЭП	*Выбрать из списка (одно):*	
		+	Требуется
			Не требуется
3.	Использование мобильного приложения	*Выбрать из списка (одно):*	
		+	DSS Client *(или мобильное приложение на базе DSS Client SDK)*
			Не требуется
4.	Взаимодействие с СЭП по защищенному протоколу TLS	*Выбрать из списка (одно):*	
			ГОСТ[2]
		+	RSA[3]

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

[2] Взаимодействие с СЭП средствами API возможно либо в случае поддержки ГОСТ TLS прикладной системой, либо с использованием прокси-шлюза с такой функциональностью.
Взаимодействие с веб-интерфейсом СЭП возможно только с помощью браузеров, поддерживающих ГОСТ TLS (например, Яндекс.Браузер, Chromium-GOST).

[3] Подключение Оператора к СЭП возможно только по ГОСТ-TLS.

<table>
<tr><td rowspan="4">5.</td><td rowspan="4">Виды сертификатов для проверки</td><td colspan="2">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td>Квалифицированные</td></tr>
<tr><td></td><td>Неквалифицированные (Сертификаты УЦ КРИПТО-ПРО)</td></tr>
<tr><td></td><td>Индивидуальный набор (оплачивается дополнительно в соответствии с условиями договора)</td></tr>
<tr><td rowspan="4">6.</td><td rowspan="4">Используемые удостоверяющие центры</td><td colspan="2">Выбрать из списка (одно или несколько):</td></tr>
<tr><td></td><td>Неаккредитованный УЦ (УЦ КриптоПро)</td></tr>
<tr><td></td><td>Аккредитованный УЦ (УЦ Такском)</td></tr>
<tr><td>+</td><td>Сторонние УЦ</td></tr>
<tr><td rowspan="3">7.</td><td rowspan="3">Использование службы штампов времени</td><td colspan="2">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td>Служба штампов времени ООО «КРИПТО-ПРО»</td></tr>
<tr><td></td><td>Другая (укажите URL-адрес службы)</td></tr>
<tr><td colspan="4">Настройки СЭП</td></tr>
<tr><td rowspan="4">8.</td><td rowspan="4">Использование PIN-кода для ключевого контейнера</td><td colspan="2">Выбрать из списка (одно):</td></tr>
<tr><td></td><td>Обязательно</td></tr>
<tr><td></td><td>Запрещено</td></tr>
<tr><td>+</td><td>Опционально (позволять задавать)</td></tr>
<tr><td colspan="4">Профиль Пользователя</td></tr>
<tr><td rowspan="20">9.</td><td rowspan="20">Состав компонентов имени (RDN) Пользователя</td><td colspan="3">Выбрать из списка (одно, или несколько); при необходимости указать значения по умолчанию для выбранных RDN:</td></tr>
<tr><td>RDN</td><td>Обязательно для заполнения</td><td>Значение по умолчанию</td></tr>
<tr><td>ОГРН</td><td></td><td></td></tr>
<tr><td>ОГРНИП</td><td></td><td></td></tr>
<tr><td>СНИЛС</td><td></td><td></td></tr>
<tr><td>ИНН ЮЛ</td><td></td><td></td></tr>
<tr><td>ИНН</td><td></td><td></td></tr>
<tr><td>Электронная почта</td><td></td><td></td></tr>
<tr><td>Страна</td><td>+</td><td>RU</td></tr>
<tr><td>Область</td><td></td><td></td></tr>
<tr><td>Город</td><td></td><td></td></tr>
<tr><td>Организация</td><td></td><td></td></tr>
<tr><td>Подразделение</td><td></td><td></td></tr>
<tr><td>Общее имя</td><td>+</td><td></td></tr>
<tr><td>Адрес</td><td></td><td></td></tr>
<tr><td>Должность</td><td></td><td></td></tr>
<tr><td>Инициалы</td><td></td><td></td></tr>
<tr><td>Имя</td><td></td><td></td></tr>
<tr><td>Фамилия</td><td></td><td></td></tr>
</table>

10.	Самостоятельное редактирование профиля Пользователем	*Выбрать из списка (одно):*	
		+	Запретить
			Разрешить
Политика учетных записей Пользователей			
11.	Используемые идентификаторы Пользователя[4]	*Выбрать из списка ниже (одно, или несколько):*	
		+	Логин
			Номер телефона
			Адрес электронной почты (e-mail)
12.	Подтверждение номера телефона Пользователя отправкой SMS	*Выбрать из списка (одно):*	
		+	Не требуется
			Требуется
13.	Подтверждение e-mail Пользователя отправкой электронного письма	*Выбрать из списка (одно):*	
		+	Не требуется
			Требуется
14.	Список операций, разрешенных для Пользователя	*Выбрать из списка ниже (одно, или несколько):*	
		+	Подпись документа
		+	Шифрование/расшифрование документа
			Создание запроса на сертификат
			Удаление сертификата
			Обновление сертификата
			Отзыв сертификата
			Приостановление действия сертификата
			Возобновление действия сертификата
		+	Смена PIN-кода для доступа к закрытому ключу сертификата
15.	Предоставить Оператору возможность управления списком разрешенных операций	*Выбрать из списка (одно):*	
			Нет
		+	Да
16.	Предоставить Пользователю возможность управления списком разрешенных операций	*Выбрать из списка (одно):*	
		+	Нет
			Да
17.	Предоставить Пользователю возможность импорта pfx	*Выбрать из списка (одно):*	
		+	Нет
			Да

[4] Выбранные идентификаторы должны быть уникальны для каждого Пользователя.

Настройки первичной аутентификации Пользователей			
18.	Методы первичной аутентификации Пользователей	*Выбрать из списка ниже (одно):*	
			Только идентификация[5]
		+	По паролю
19.	Разрешить Пользователям самостоятельное изменение настроек первичной аутентификации[6]	*Выбрать из списка (одно):*	
		+	Нет
			Да
Политики долговременных паролей			
20.	Длина долговременных паролей (*от 1 до 256 символов*)	8 символов	
21.	Сложность долговременных паролей	*Выбрать из списка (одно):*	
		+	Цифры и буквы в разном регистре
			Цифры и буквы в разном регистре и специальные символы
			Цифры и буквы
			Только цифры
			Парольные фразы[7]
22.	Максимальное количество попыток ввода долговременного пароля до блокирования учётной записи	*Выбрать из списка (одно):*	
		+	5 (можно указать собственное значение)
			0 (Блокирование отключено)
23.	Срок действия долговременного пароля (*в днях*)	*Выбрать из списка (одно):*	
		+	Срок действия не ограничен
			Указать количество дней
24.	Требовать смену пароля Пользователя при первом входе в СЭП[8]	*Выбрать из списка (одно):*	
		+	Не требовать
			Требовать

[5] Требуется использование вторичного фактора аутентификации (мобильное приложение или одноразовый пароль – п.3 и п.25).

[6] Требуется использование вторичного фактора аутентификации (мобильное приложение или одноразовый пароль – п.3 и п.25).

[7] Парольные фразы – механизм генерации стойких и легко запоминаемых долговременных паролей. Сложность парольной фразы по умолчанию – 3 слова (максимум – 4 слова).

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

Политики вторичной аутентификации			
25.	Альтернативные методы вторичной аутентификации Пользователей[9]	*Выбрать из списка (одно):*	
			Одноразовый пароль по SMS
			Одноразовый пароль по EMAIL
			Генератор одноразовых паролей[10]
26.	Список операций, требующих подтверждения	*Выбрать из списка ниже (одно, или несколько):*	
		+	Подпись документа
		+	Подпись пакета документов
		+	Расшифрование документа
		+	Создание запроса на сертификат
		+	Удаление сертификата
		+	Смена PIN-кода для доступа к закрытому ключу сертификата
		+	Создание запроса на обновление сертификата
		+	Создание запроса на отзыв сертификата
		+	Создание запроса на приостановление действия сертификата
		+	Возобновление действия сертификата
		+	Выпуск маркера безопасности («вход» Пользователя)[11]
27.	Разрешить Пользователям самостоятельное изменение настроек вторичной аутентификации[12]	*Выбрать из списка (одно):*	
		+	Нет
			Да
28.	Предоставить Оператору возможность управления списком операций, требующих подтверждения[13]	*Выбрать из списка (одно):*	
			Нет
		+	Да

[9] Стойким способом вторичной аутентификации является только мобильное приложение (см. п.3). Включение альтернативных методов аутентификации одновременно с мобильным приложением не рекомендуется.

[10] Поддерживаются программные (например, Яндекс.Ключ, Google Authenticator, Microsoft Authenticator) и аппаратные (токены, брелоки и др.) генераторы одноразовых паролей, поддерживающие спецификации OATH (TOTP или HOTP).

[11] Если в методах первичной аутентификации Пользователей (п. 18) включена только идентификация, то данная операция должна требовать подтверждения, в противном случае будет возможна работа только через API с использованием конфиденциальных клиентов OAuth, а веб-интерфейс пользователя и работа через КриптоПро Cloud CSP будут недоступны.

[12] Не рекомендуется разрешать Пользователям самостоятельно изменять настройки вторичной аутентификации, если в качестве метода первичной аутентификации выбрана только идентификация (п. 18), т.к. в результате может возникнуть небезопасная конфигурация аутентификации.

[13] Не рекомендуется разрешать Оператору самостоятельно изменять настройки вторичной аутентификации, если в качестве метода первичной аутентификации Пользователей выбрана только идентификация (п. 18), т.к. в результате может возникнуть небезопасная конфигурация аутентификации.

29.	Предоставить Пользователю возможность управления списком операций, требующих подтверждения	*Выбрать из списка (одно):*	
		+	Нет
			Да
Настройки APIv2[14]			
30.	Максимальное время хранения документов (до 7 дней)	3 дня	
31.	Срок действия QR-кода для инициализации мобильного устройства	7 дней	
32.	Список операций, разрешенных для выполнения из мобильного приложения	*Выбрать из списка (одно, или несколько):*	
		+	Подпись документа
			Установка сертификата
			Создание запроса на сертификат
33.	Предоставить возможность архивации ключей, хранящихся в мобильном приложении	*Выбрать из списка (одно):*	
			Нет
		+	Да
Политики одноразовых паролей и паролей мобильных приложений			
34.	Длина одноразовых паролей (*от 1 до 256 символов*)	6 символов	
35.	Сложность одноразовых паролей	*Выбрать из списка (одно):*	
		+	Только цифры
			Цифры и буквы
			Цифры и буквы в разном регистре
			Цифры и буквы в разном регистре и специальные символы
36.	Максимальное количество попыток ввода одноразового пароля до блокирования учётной записи	*Выбрать из списка (одно):*	
		+	3 (можно указать собственное значение)
			Блокирование отключено
37.	Отправка кодов активации для QR-кодов мобильных приложений[15]	*Выбрать из списка (одно):*	
		+	Требуется
			Не требуется
38.	Сложность паролей для мобильных приложений	*Выбрать из списка (одно):*	
		+	Без пароля/любой пароль
			Минимум 6 символов
			Минимум 8 символов, буквы в разном регистре
			Минимум 8 символов, цифры и буквы в разном регистре

[14] Заполняется при условии, если выбран метод вторичной аутентификации DSS Client (п. 3).
[15] Отправлять код активации по SMS или E-mail.

<table>
<tr><td colspan="5">Политики операций[16]</td></tr>
<tr><td>39.</td><td>Время жизни операции в секундах[17]</td><td colspan="3">300 (можно указать собственное значение, но не более 3 суток)</td></tr>
<tr><td colspan="5">Параметры OAuth</td></tr>
<tr><td rowspan="3">40.</td><td rowspan="3">Адрес перенаправления redirect_uri[18]</td><td colspan="3">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td colspan="2">Значение по умолчанию</td></tr>
<tr><td></td><td colspan="2">(указать адрес перенаправления)</td></tr>
<tr><td colspan="5">Группы Пользователей СЭП</td></tr>
<tr><td rowspan="5">41.</td><td rowspan="5">Информация о группах пользователей и их Операторах</td><td colspan="3">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td colspan="2">Группа пользователей по умолчанию</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Собственные группы пользователей (указать в таблице ниже)</td></tr>
<tr><td>Имя группы</td><td>Описание группы</td><td>Логин Оператора группы</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="5">Настройки уведомлений</td></tr>
<tr><td>42.</td><td>Перечень событий для рассылки уведомлений Пользователям и Операторам по электронной почте (email)[19]</td><td colspan="3">Выбрать значения уведомлений Операторов и Пользователей СЭП в таблице (вкладка NEW)), размещенной по адресу:
http://dss.cryptopro.ru/reglament/ОповещенияСЭП.xlsx</td></tr>
<tr><td rowspan="6">43.</td><td rowspan="6">Перечень адресов электронной почты (email) для рассылки уведомлений Операторам о событиях СЭП</td><td colspan="3">Указать адреса электронной почты (e-mail) Операторов СЭП:</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="5">Другие настройки</td></tr>
<tr><td>44.</td><td>Другие настройки[20]</td><td colspan="3"></td></tr>
</table>

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

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

М.П.

[16] Операция – это любое действие с закрытым ключом (сертификатом) Пользователя (например, подпись документов, создание запроса на сертификат, расшифрование и т.п.) и аутентификация Пользователя в СЭП.

[17] Время, в течение которого Пользователь должен подтвердить операцию.

[18] Адрес перенаправления результата запроса в виде кода авторизации. Можно указать адрес выделенного HTTP-сервиса для обработки URI перенаправления.

[19] Перечень событий для рассылки уведомлений предоставляется в электронном виде.

[20] Заполняется по согласованию.

Приложение № 8 к Регламенту Сервиса ЭП
(Форма заявления на подключение SMS-шлюза)

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

по Договору №_____ от ___.___._____ г.

_____
(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 № 9 к Регламенту Сервиса ЭП
(Форма заявления на подключение Стороннего центра идентификации
по протоколу WS-Federation)

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

по Договору №_____ от ___.___._____ г.

_____
(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 СЦИ
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.

(Форма заявления на подключение Стороннего центра идентификации)
по протоколу OpenId Connect 1.0)

Заявление на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО» по протоколу OpenId Connect 1.0

по Договору №_____ от ___.___._____ г.

_____
(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 СЦИ
3.	Адрес СЦИ	URL-адрес взаимодействия с СЦИ (необходим при web-доступе пользователей)
4.	JwksUri	Адрес точки распространения набора ключей
5.	Краткое описание СЦИ	Краткие сведения о подключаемом СЦИ
6.	ClientId	Идентификатор oauth-клиента
7.	Срок действия сертификата СЦИ	Дата начала и окончания действия сертификата Стороннего ЦИ (NotBefore, NotAfter)
8.	Отпечаток сертификата СЦИ	Хеш сертификата СЦИ (sha1)
9.	Режим регистрации пользователей СЦИ в СЭП	Автоматический (при первичном обращении к СЭП)/Оператором СЦИ
10.	Отображаемое наименование группы пользователей (1).	Опционально. Если не указан – используется группа по умолчанию для всех пользователей. Указать для всех планируемых групп в дополнительных пунктах.
		Уникальный идентификатор группы пользователей (1).
11.	ФИО	Работник Уполномоченной Организации, ответственный за подключение и функционирование СЦИ, и его контактные данные:
12.	Подразделение	Ответственного работника Уполномоченной организации
13.	Адрес электронной почты	Ответственного работника Уполномоченной организации
14.	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).
2. ClientSecret – Значение секрета oauth-клиента, идентификатор которого указан в пункте 6.

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

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

М.П.

Приложение № 10 к Регламенту Сервиса ЭП
(Форма заявления на регистрацию Оператора СЦИ)

Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации

по Договору №_____ от ___.___._____ г.

_____
(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

(уазывается при необходимости такой рассылки)

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

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

М.П.

Приложение № 11 к Регламенту Сервиса ЭП
(Форма заявления на подключение Удостоверяющего центра)

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

по Договору №_____ от ___.___._____ г.

_____
(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 № 12 к Регламенту Сервиса ЭП
(Форма запроса на предоставление информации для разбора конфликтной ситуации)
(Форма заявления на подтверждение подлинности ЭП)

Запрос информации для разбора конфликтной ситуации

по Договору №_____ от ___.___._____ г.

_____
(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 сведения)

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.

(Форма заявления на подтверждение подлинности ЭП)

Заявление на подтверждение подлинности электронной подписи в электронном документе

по Договору №_____ от ___.___._____ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

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

3. Время[21] на момент наступления которых требуется подтвердить подлинность ЭП: «_____:_____» «_____/_____/_____»;
час минута день месяц год

Оператор СЭП
ООО «КРИПТО-ПРО» _____/_____/

«____» _____ 20____ г.

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

«____» _____ 20____.

М.П.

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

Приложение № 13 к Регламенту Сервиса ЭП
(Рекомендуемая 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, 105037, г. Москва, вн. тер. г. муниципальный округ Измайлово, Измайловский проезд, д. 10, к. 2, помещ. 4/1) 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, 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_____ /_____/

Приложение №14 к Регламенту Сервиса ЭП
(Форма сведений из сертификата ключа проверки электронной подписи)

Сведения из сертификата ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан:
Фамилия Имя Отчество
Кем выдан:
УЦ КРИПТО-ПРО
Действителен с 31 января 2021 г. 21:30:28 UTC по 31 января 2036 г. 21:30:28 UTC
Версия: 3 (0x2)
Серийный номер: 14F5 9CF2 0000 0000 003A
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2012
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Издатель сертификата: CN = УЦ КРИПТО-ПРО, O = ООО КРИПТО-ПРО, L = Москва, C = RU, E = cpca@cryptopro.ru
Срок действия:
Действителен с: 15 мая 2023 г. 12:03:00 UTC
Действителен по: 15 мая 2024 г. 12:12:00 UTC
Владелец сертификата: CN = Фамилия, Имя, Отчество, email = a@b.ru
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2012
Идентификатор: 1.2.643.2.2.20
Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 56BD CA83 3029 0673 CA83 3381 16D4 AF10 C3D6 9A75
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=50AA 3E1E 4186 F8DC 3585 6E11 2C11 D9E3 0A91 7AD7 Поставщик сертификата: Адрес каталога: CN = УЦ КРИПТО-ПРО, O = ООО КРИПТО-ПРО, L = Москва, C = RU, E = cpca@cryptopro.ru Серийный номер сертификата=29D1 B0C8 C311 ACAE 48DB AAB1 3687 CEFC
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2012
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Значение: 826C DDFB 331C 58C5 FD3D 9233 4A1D 2D7A B973 387C 8E8A DD3D 6FCE 0573 508A 3DC4 B29F 5961 FB6C D1EB 1B40 37C7 8473 5B0F FECA 5E38 EA0C 3890 C77A C97E BD18 873A

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

Приложение № 15 к Регламенту Сервиса ЭП
(Форма заявления на подключение дополнительного сервиса проверки электронной подписи к Сервису электронной подписи ООО «КРИПТО-ПРО»)

Заявление на подключение дополнительного сервиса проверки электронной подписи к Сервису электронной подписи ООО «КРИПТО-ПРО»

по Договору №_____ от ___.___._____ г.

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

просит подключить дополнительный сервис проверки электронной подписи к Сервису электронной подписи ООО «КРИПТО-ПРО» в соответствии с указанными в настоящем заявлении сведениями:

№ п/п	Параметр СЭП	Настраиваемое значение параметра СЦИ
1.	Наименование экземпляра	
2.	Режим проверки сертификатов[22]	Опционально. Если не указан – используется online проверка.
3.	Проверка на соответствия полей сертификата установленной форме.	
4.	Перечень Удостоверяющих центров – издателей проверяемых сертификатов	

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

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

М.П.

[22] Возможные режимы проверки и описание указаны в документации: https://dss.cryptopro.ru/docs/svs/adminguide/set/certstatus.html