Утвержден
Приказом ООО «КРИПТО-ПРО» № 1
от «10» января 2023 г.

РЕГЛАМЕНТ

по выпуску и управлению квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)

Редакция № 2

г. Москва
2023

1. Сведения об Исполнителе

Общество с ограниченной ответственностью «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 29.01.2003 г.).

Исполнитель осуществляет свою деятельность на территории Российской Федерации 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 нахождения и для корреспонденции: 127018, г. Москва, ул. Сущевский Вал, д. 18
Банковские реквизиты (наименование банка, БИК, р/с, к/с):

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

ИНН/КПП: 7717107991/771901001
ОГРН: 1037700085444
Контактные телефоны, факс, адрес электронной почты:
тел./факс (495) 995-48-20; e-mail: qca@cryptopro.ru, info@cryptopro.ru

2. Термины и определения

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

Веб-интерфейс, предоставляемый Исполнителем – интерфейс взаимодействия Пользователя Удостоверяющего центра 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-узле Исполнителя.

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

Заявитель – юридическое лицо, индивидуальный предприниматель, иной хозяйствующий субъект, физическое лицо, обращающееся с соответствующим заявлением к Исполнителю на выпуск сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

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

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

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

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

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

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

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, соответствующий содержательной части сертификата ключа проверки электронной подписи и заверенный в соответствии с порядком заверения копий документов, установленным у *Исполнителя* и *Уполномоченной организации*. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

Многофакторная аутентификация - процедура проверки подлинности Пользователя Удостоверяющего центра при осуществлении доступа с использованием двух и более уникальных характеристик, известных или присущих только Пользователю Удостоверяющего центра (факторов аутентификации). При управлении доступом к Сервису электронной подписи для первичной аутентификации Пользователя Удостоверяющего Центра используется постоянно действующий пароль, самостоятельно определяемый Пользователем Удостоверяющего центра, для вторичной аутентификации – ключ аутентификации в мобильном приложении СЭП на устройствах пользователей; одноразовый пароль,

формируемый Сервисом электронной подписи и высылаемый Пользователю Удостоверяющего центра в информационном сообщении на номер мобильного телефона, указанный Пользователем Удостоверяющего центра при регистрации, или OTP-токеном, выдаваемый Оператором УЦ по заявлению Пользователя Удостоверяющего центра. Уполномоченная организация вправе использовать дополнительные факторы аутентификации для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи совместно с собственным Сторонним центром идентификации.

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

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

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

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

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

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем квалифицированного сертификата ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец сертификата ключа проверки электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица, присоединившееся к Регламенту Уполномоченной организации.

Порядок реализации функций Удостоверяющего центра – документ, который регулирует условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра, а также правила пользования услугами Удостоверяющего центра, который размещается на официальном сайте Удостоверяющего центра.

Прикладной интерфейс, предоставляемый Исполнителем (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 с использованием средств криптографической защиты информации, совместимых со средствами Исполнителя.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Сторонний центр идентификации – система аутентификации Уполномоченной организации, подключаемая к Сервису электронной подписи по стандартным протоколам и используемая Уполномоченной организацией для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи.

Тестовый сертификат – временный неквалифицированный сертификат ключа проверки электронной подписи, выданный тестовым удостоверяющим центром, не имеющий юридической силы и предназначенный исключительно для тестирования функциональности СЭП.

Удостоверяющий центр – аккредитованный в соответствии с Федеральным законом от 06.04.2011 г. №63-ФЗ «Об электронной подписи» удостоверяющий центр, заключивший с Исполнителем договор оказания услуг аккредитованного удостоверяющего центра. Удостоверяющий центр осуществляет свою деятельность в соответствии с Порядком реализации функций Удостоверяющего центра. Указанный Порядок размещается на официальном сайте Удостоверяющего центра.

Уполномоченная организация – юридическое лицо, заключившее с Исполнителем договор, наделённое полномочиями по принятию решений по выпуску и управлению квалифицированных сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра и управлению доступом к Сервису электронной подписи.

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

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

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

Cryptographic Message Syntax (CMS) – стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом применения российских криптографических алгоритмов.

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

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

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий Центр осуществляют свою работу в соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа проверки электронной подписи.

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

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

SMS-шлюз – служба рассылки информационных сообщений Уполномоченной Организации, подключаемая к Сервису электронной подписи и используемая Уполномоченной организацией для отправки Пользователям Удостоверяющего центра одноразовых паролей и уведомлений о выполняемых в СЭП операциях.

Принятие Уполномоченной организацией решения по выпуску квалифицированного сертификата ключа проверки электронной подписи – это действия Оператора СЭП, необходимые для формирования и отправки в Удостоверяющий центр заявок в электронной форме на создание сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, с помощью средств, предоставляемых Исполнителем, и сертификата ключа проверки электронной подписи Оператора СЭП.

Принятие Уполномоченной организацией решения по управлению квалифицированным сертификатом ключа проверки электронной подписи – это действия Оператора СЭП, необходимые для формирования и отправки в Удостоверяющий центр заявок в форме, установленной настоящим Регламентом, на установление статуса, подтверждения подлинности, прекращение действия квалифицированного сертификата ключа проверки электронной подписи Пользователей Удостоверяющего центра.

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

3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент по выпуску и управлению квалифицированными сертификатами ключей проверки электронной подписи (Схема обслуживания: распределенная с оператором СЭП), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации в области применения электронной подписи.

3.1.2. Сторонами Регламента (далее - Стороны) являются Исполнитель - ООО «КРИПТО-ПРО», и Уполномоченная организация.

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

3.2. Применение Регламента

3.2.1. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

3.2.2. В случае противоречия и/или расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

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

3.3. Изменение Регламента

3.3.1. Внесение изменений в Регламент, включая приложения к нему, производится 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://q.cryptopro.ru/reglament/reglamentoperdssca.pdf.

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

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

3.3.5. Любые изменения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений в силу.

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

4. Предоставление информации

4.1. 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:

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

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

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

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

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

Уполномоченная организация подтверждает, что ею получено письменное согласие субъектов персональных данных, чьи персональные данные содержатся в представленных Уполномоченной организацией Исполнителю документах, на обработку Исполнителем этих персональных данных по поручению Уполномоченной организации в указанных выше целях, а также гарантирует, что содержащие персональные данные документы будут представляться Уполномоченной организацией Исполнителю в соответствии с настоящим Регламентом с согласия субъектов персональных данных, чьи персональные данные содержатся в таких документах. Письменное согласие Оператора СЭП на обработку его персональных данных Исполнителем оформляется в форме Заявления на регистрацию Оператора СЭП (Приложение №1 к настоящему Регламенту). Письменное согласие Пользователя Удостоверяющего центра на обработку его персональных данных оформляется в заявлении на выпуск квалифицированного сертификата ключа проверки ЭП согласно Порядку реализации функций удостоверяющего центра и в иных документах, определяемых Уполномоченной организацией согласно Регламента Уполномоченной организации. Уполномоченная организация несет все неблагоприятные последствия, связанные с неполучением Уполномоченной организацией таких согласий.

Уполномоченная организация подтверждает, что ею получено письменное согласие субъектов персональных данных, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых они являются, относятся к персональным данным, предоставление которых разрешено в целях надлежащего и своевременного получения услуг, связанных с выпуском квалифицированного сертификата ключа проверки электронной подписи.

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 и иных неправомерных действий в отношении персональных данных определяются Удостоверяющим центром самостоятельно с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Права и обязанности сторон

5.1. Исполнитель обязан:

5.1.1. Организовать свою работу по рабочим дням. Исполнитель обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

5.1.2. Зарегистрировать Оператора СЭП по заявлению на регистрацию в СЭП в соответствии с порядком, определенным в настоящем Регламенте.

5.1.3. Предоставить аутентифицированным Пользователям Удостоверяющего центра, получившим сертификат ключа проверки электронной подписи в соответствии с Регламентом Уполномоченной организации, доступ к СЭП и обеспечить круглосуточное функционирование СЭП в режиме 24x7. Восстановить функционирование СЭП в течение 1 (одного) часа рабочего времени в случае проведения плановых регламентных работ или возникновения внештатных ситуаций. Доступные Пользователям функциональные возможности СЭП приведены в Приложении № 6 к настоящему Регламенту.

5.1.4. Использовать в составе СЭП средства криптографической защиты информации и электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» для создания и хранения ключей электронной подписи Пользователей Удостоверяющего центра.

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

5.1.6. Обеспечить прекращение действия сертификата ключа проверки электронной подписи Оператора СЭП по соответствующему заявлению на прекращение действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в Регламенте.

5.1.7. Обеспечить прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в соответствии с порядком, определенным в Регламенте.

5.1.8. Предоставить Уполномоченной организации на согласование и утверждение перечень параметров функционирования СЭП для настройки доступа Операторов СЭП и Пользователей УЦ по форме в соответствии с Приложением № 7 к настоящему Регламенту.

5.1.9. Предоставить Уполномоченной организации необходимые права для:

5.1.9.1. осуществления регистрации пользователей в СЭП, формированию и отправке в Удостоверяющий центр заявок в электронной форме на выпуск и управление сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра;

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

5.1.9.3. подключения к СЭП Стороннего центра идентификации в соответствии с настоящим Регламентом;

5.1.9.4. подключения SMS-шлюза Уполномоченной организация к СЭП в соответствии с настоящим Регламентом.

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

5.1.9.6. подключения Информационных систем Уполномоченной организации к СЭП с использованием Прикладного интерфейса, предоставляемого Исполнителем;

5.1.10. Зарегистрировать в СЭП Оператора подключенного Стороннего центра идентификации Уполномоченной организации в соответствии с заявлением по форме Приложения №8 к настоящему Регламенту, полученного от Уполномоченной организации.

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

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

5.1.13. Не позже, чем за 30 (Тридцать) рабочих дней информировать Уполномоченную организацию о проведении обновления программного обеспечения СЭП, предоставить доступ к тестовой версии СЭП с обновленным программным обеспечениеми соответствующую ему руководство разработчика на программное обеспечение. Информирование осуществляется путем отправки электронного сообщения по электронному адресу, указанному в действующем сертификате ключа проверки электронной подписи Оператора СЭП.

5.2. Уполномоченная организация обязана:

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

5.2.2. После проведения проверки с использованием тестовых сертификатов ключей проверки электронной подписи согласовать и подписать предоставленный Исполнителем перечень настроенных параметров функционирования СЭП для доступа Операторов СЭП и Пользователей Удостоверяющего центра по форме, установленной в Приложении № 7 к настоящему Регламенту.

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

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

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

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

5.2.7. По письменному запросу предоставить Исполнителю письменное согласие Пользователя Удостоверяющего центра на получение информационных сообщений на номер

мобильного телефона Пользователя Удостоверяющего центра в сроки, установленные в запросе Исполнителя.

5.2.8. Установленным в Уполномоченной организации порядке заверять копии сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром по заявкам Оператора СЭП, являющимся полномочным лицом Уполномоченной организации.

5.2.9. При приёме заявлений на выпуск сертификатов ключей проверки электронной подписи, а также при вручении сертификатов ключей проверки электронной подписи Пользователю Удостоверяющего центра осуществлять фото и/или видео фиксацию Пользователя Удостоверяющего центра в момент его идентификации. Требования к порядку и процедурам фото и/или видео фиксации размещаются на сайте Удостоверяющего центра.

5.2.10. Оператор СЭП, являющийся полномочным представителем Уполномоченной организации обязан:

5.2.10.1. При взаимодействии со средствами обеспечения деятельности Исполнителя использовать только те средства, которые были предоставлены Исполнителем.

5.2.10.2. Обеспечить конфиденциальность ключей электронных подписей.

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

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

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

5.2.10.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр или Исполнителю, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия квалифицированного сертификата ключа проверки электронной подписи до момента времени официального уведомления о прекращении действия сертификата ключа проверки электронной подписи, либо об отказе в прекращении действия сертификата ключа проверки электронной подписи.

5.2.10.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, действие которого прекращено.

5.2.10.8. Для направления Исполнителю заявок на создание и проверку усиленных квалифицированных электронных подписей, создание ключей электронной подписи и ключей проверки электронной подписи использовать СЭП и средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

5.3. Исполнитель имеет право:

5.3.1. Отказать в выпуске сертификата ключа проверки электронной подписи Оператора СЭП в случае ненадлежащего оформления заявления на выпуск квалифицированного сертификата ключа проверки электронной подписи.

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

5.3.3. Отказать в прекращении действия сертификата ключа проверки электронной подписи Оператора СЭП в случае ненадлежащего оформления соответствующего заявления на прекращение, приостановление и возобновление действия квалифицированного сертификата ключа проверки электронной подписи.

5.3.4. Отказать в прекращении действия сертификата ключа проверки электронной подписи Оператора СЭП в случае, если истек установленный срокдействия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи.

5.3.5. В одностороннем порядке приостановить подключение Оператора СЭП к СЭП с обязательным уведомлением Оператора СЭП и указанием причин приостановления подключения к СЭП.

5.3.6. Отказать в выпуске и управлении сертификатами ключей проверки электронной подписи по заявкам Оператора СЭП до момента получения от Уполномоченной организации подписанного перечня параметров функционирования СЭП для настройки прав доступа Операторов СЭП и Пользователей Удостоверяющего центра по форме, указанной в Приложении № 7 к настоящему Регламенту.

5.3.7. Отказать в подключении Стороннего центра идентификации Уполномоченной организации в случае ненадлежащего оформления заявления на подключение Стороннего центра идентификации, оформляемого в соответствии с Приложением №4 к настоящему Регламенту.

5.3.8. Отказать в подключении SMS-шлюза Уполномоченной организации в случае ненадлежащего оформления заявления на подключение SMS-шлюза, оформляемого в соответствии с Приложением № 5 к настоящему Регламенту.

5.3.9. Отказать в регистрации Оператора Стороннего центра идентификации до получения надлежащим образом оформленного заявления на подключение Стороннего центра идентификации Уполномоченной организации по форме, установленной в Приложении №4 к настоящему Регламенту, или в случае ненадлежащего оформления заявления на регистрацию Оператора Стороннего центра идентификации, оформляемого в соответствии с Приложением № 8 к настоящему Регламенту.

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

5.4. Уполномоченная организация имеет право:

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

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

5.4.3. Подать Исполнителю заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации по форме, установленной Приложением № 8 к настоящему Регламенту.

5.4.4. Осуществить в соответствии с п.8.8 настоящего Регламента подключение к СЭП собственного SMS-шлюза для отправки Пользователям Удостоверяющего центра информационных сообщений с одноразовыми паролями и уведомлениями о выполняемых СЭП операциях с использованием принадлежащих им ключей электронной подписи.

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

5.4.6. Предоставлять Пользователям Удостоверяющего центра возможность установки мобильного приложения СЭП на устройства Пользователей Удостоверяющего центра и создавать им ключ аутентификации для выполнения многофакторной аутентификации при осуществлении доступа к СЭП.

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

5.4.8. Делегировать Пользователям Удостоверяющего центра право подачи заявки Исполнителю на выпуск и управление своими квалифицированными сертификатами ключей проверки электронной подписи посредством Веб- или Прикладного интерфейса СЭП, предоставляемых Исполнителем. Предоставленные Уполномоченной организацией права Пользователей Удостоверяющего центра определяются параметрами функционирования СЭП в соответствии с Приложением № 7 к настоящему Регламенту и соглашением, заключённым Уполномоченной организацией и Пользователем Удостоверяющего центра. Уполномоченная организация несет всю ответственность за создаваемые Удостоверяющим центром квалифицированные сертификаты ключей проверки электронной подписи по заявкам Пользователей Удостоверяющего центра в соответствии с предоставленными им Уполномоченной организацией правами.

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

5.4.10. Оператор СЭП имеет право:

5.4.10.1. Получить копию сертификата ключа проверки электронной подписи Оператора СЭП на бумажном носителе, заверенную установленным у Исполнителя порядком.

5.4.10.2. Заверять собственноручной подписью копии сертификатов ключей проверки электронной подписи, решение по выпуску которых было принято Оператором СЭП.

5.4.10.3. Принимать решения о подаче Исполнителю заявки на выпуск сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.4.10.4. Принимать решения о подаче Исполнителю заявок на прекращение действия сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, созданных Удостоверяющим центром по заявкам Оператора СЭП.

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

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

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

5.4.10.8. Обратиться к Исполнителю с заявлениями на выполнение Исполнителем действий, установленных настоящим Регламентом.

6. Ответственность сторон

6.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

6.2. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

6.3. 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 Оператора СЭП.

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

6.5. Вся ответственность по обеспечению конфиденциальности ключа аутентификации при передаче Пользователю Удостоверяющего центра для использования в мобильном приложении СЭП возлагается на Уполномоченную организацию.

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

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

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

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

7. Разрешение споров

7.1. Сторонами в споре, в случае его возникновения, считаются Исполнитель и Уполномоченная организация.

7.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.

7.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

7.4. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в Арбитражном суде г. Москвы.

8. Порядок предоставления и пользования услугами

8.1. Общий порядок пользования услугами Исполнителя

Уполномоченная организация в лице Оператора СЭП осуществляет приём заявлений, принятие решений по выпуску и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра в соответствии с Порядком реализации функций Удостоверяющего центра после подключения Оператора СЭП к СЭП.

Исполнитель осуществляет действия по формированию ключей электронной подписи, выпуску и управлению сертификатами ключей проверки электронной подписи по заявкам, направленным Оператором СЭП в электронной форме, формируемым в СЭП Оператором СЭП.

Для взаимодействия с Исполнителем Уполномоченная организация в лице Оператора СЭП должна стать владельцем сертификата ключа проверки электронной подписи.

Формирование ключей электронной подписи, выпуск и управление сертификатами Операторов СЭП осуществляется в соответствии с настоящим разделом Регламента.

8.2. Регистрация Оператора СЭП и выпуск сертификата ключа проверки электронной подписи Оператора СЭП.

Регистрация Оператора СЭП осуществляется на основании заявления регистрацию Оператора СЭП (оформляется по форме Приложения №1 к настоящему Регламенту) и доверенности Оператора СЭП (оформляется по форме Приложения №2 к настоящему Регламенту).

Процедура регистрации Оператора СЭП включает выпуск Оператору СЭП сертификата ключа проверки электронной подписи. Выпуск сертификата ключа проверки электронной подписи Оператора СЭП осуществляется на основании заявления на выдачу сертификата ключа проверки электронной подписи Оператора СЭП. Форма заявления на выдачу сертификата ключа проверки электронной подписи Оператора СЭП устанавливается Порядком реализации функций Удостоверяющего центра.

Предоставление заявительных документов для регистрации и для выпуска сертификата ключа проверки электронной подписи Оператора СЭП, а также получение ключа электронной подписи и сертификата ключа проверки электронной подписи Оператора СЭП, осуществляется Оператором СЭП лично.

Исполнитель на основе предоставленных заявительных документов выполняет действия, необходимые для выпуска сертификата ключа проверки электронной подписи Оператора СЭП.

Исполнитель распечатывает на бумажном носителе информацию, содержащуюся в выпущенном сертификате ключа проверки электронной подписи, представленную в виде копии сертификата ключа проверки электронной подписи, оформленной по форме Приложения № 3 к настоящему Регламенту. Оператор СЭП под расписку ознакамливается с информацией из сертификата ключа проверки электронной подписи.

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

Выпуск сертификата ключа проверки электронной подписи Оператору СЭП осуществляется Исполнителем в день прибытия заявителя в случае отсутствия со стороны Оператора СЭП нарушений положений настоящего Регламента. День прибытия заявителя согласовывается с Исполнителем. Исполнитель вправе отказать в выпуске сертификата ключа проверки электронной подписи Оператору СЭП по заявлениям, поступившим к Исполнителю без согласования дня прибытия заявителя.

8.3. Прекращение действия сертификата ключа проверки электронной подписи Оператора СЭП

Прекращение действия сертификата ключа проверки электронной подписи Оператора СЭП производится в следующих случаях:

- при прекращении действия настоящего Регламента в отношении Уполномоченной организации по усмотрению Исполнителя;

- по заявлению владельца сертификата ключа проверки электронной подписи;
- в связи с аннулированием сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу;
- по истечении срока действия сертификата ключа проверки электронной подписи;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи.

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

Подача заявления на прекращение действия сертификата ключа проверки электронной подписи Оператора СЭП осуществляется по форме, установленной Порядком реализации функций Удостоверяющего центра и может быть осуществлена посредством отправления Исполнителю данного заявления почтовой или курьерской связью.

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

В случае отказа в прекращении действия сертификата ключа проверки электронной подписи Оператора СЭП Исполнитель уведомляет об этом Оператора СЭП с указанием причин отказа.

При принятии положительного решения о прекращении действия сертификата ключа проверки электронной подписи Оператора СЭП – действие сертификата прекращается.

8.4. Подключение Информационной системы Уполномоченной Организации к Сервису электронной подписи

Исполнитель предоставляет Уполномоченной организации Прикладной интерфейс подключения к Сервису электронной подписи в соответствии с руководством разработчика на программное обеспечение СЭП. Защита передаваемых от Информационной системы к Сервису электронной подписи данных осуществляется в соответствии с требованиями Уполномоченной Организации с использованием СКЗИ, совместимых со средствами Исполнителя.

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

Подключение Стороннего центра идентификации Уполномоченной организации к Сервису электронной подписи осуществляется в соответствии с документацией на программное обеспечение СЭП по заявлению на подключение Стороннего центра идентификации к Сервису электронной подписи ООО «КРИПТО-ПРО», оформляемому по форме Приложения №4 к настоящему Регламенту, от Уполномоченной Организации. Заявление на подключение Стороннего центра идентификации к Сервису электронной подписи направляется Исполнителю курьерской или почтовой связью. Вместе с заявлением на подключение Стороннего центра идентификации к Сервису электронной подписи на носителе информации передается сертификат, используемый для проверки подписи SAML-токенов,передаваемых от Стороннего центра идентификации.

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

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

Заявление на подключение Стороннего центра идентификации к Сервису электронной подписи и сертификат Стороннего центра идентификации могут быть отправлены Исполнителю в электронной форме, подписанные электронной подписью Оператора СЭП и руководителя Уполномоченной организации с использованием сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

Регистрацию Оператора СЦИ в СЭП выполняет Исполнитель после получения заявления на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации, оформленного по форме Приложения № 8 к настоящему Регламенту и доверенности Оператора Стороннего центра идентификации Уполномоченной организации. Форма доверенности Оператора Стороннего центра идентификации Уполномоченной организации устанавливается в Приложении № 9 к настоящему Регламенту. Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации и доверенность Оператора Стороннего центра идентификации Уполномоченной организации направляются Исполнителю курьерской или почтовой связью.

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

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

Подключение SMS-шлюза Уполномоченной Организации к Сервису электронной подписи осуществляется в соответствии с документацией на программное обеспечение СЭП по заявлению на подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи, оформляемому по форме Приложения № 5 к настоящему Регламенту, полученному от Уполномоченной Организации. Заявление на подключение SMS- шлюза Уполномоченной организации к Сервису электронной подписи направляется Исполнителю курьерской или почтовой связью.

Заявление на подключение SMS-шлюза Уполномоченной организации к Сервису электронной подписи может быть отправлено Исполнителю в электронной форме, подписанное электронной подписью Оператора СЭП и руководителя Уполномоченной организации с использованием сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

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

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

Регистрация Пользователей Удостоверяющего центра, принятие решений по выпуску сертификатов ключей проверки электронной подписи Пользователей УЦ и управлению сертификатами ключей проверки электронной подписи Пользователей УЦ, формирование копий сертификатов ключей проверки электронной подписи Пользователей УЦ производится Оператором СЭП.

Действия по выпуску сертификатов ключей проверки электронной подписи Пользователя УЦ, прекращению действия сертификатов ключей проверки электронной подписи Пользователя УЦ, приостановлению и возобновлению действий сертификатов ключей проверки электронной подписи Пользователя УЦ осуществляется в соответствии с настройками параметров функционирования СЭП, определенных в Перечне параметров функционирования Сервиса электронной подписи для настройки доступа Операторов СЭП и Пользователей УЦ, оформляемом по форме Приложения № 7, на основании заявок в электронной форме внутреннего формата СЭП, направляемых Оператором СЭП и (или) Пользователями Удостоверяющего центра с использованием 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 Удостоверяющего центра;
- 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 УЦ подтверждена с использованием ключа аутентификации в мобильном приложении СЭП или СКЗИ «КриптоПро CSP» на рабочем месте Пользователя УЦ или одноразовым паролем, переданного заявителю от СЭП посредством информационного сообщения или сформированным им с использованием OTP- токена, полученного от Оператора СЭП.

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

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

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

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

8.8. Предоставление Исполнителем сервисов Службы актуальных статусов сертификатов и Службы штампов времени при использовании СЭП

Исполнитель предоставляет актуальную информацию о статусе сертификатов ключа проверки электронной подписи при использовании СЭП посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра посредством СЭП формирует и предоставляет этим Пользователям Удостоверяющего центра OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов). OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭП Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;
- Сертификат ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности ЭП OCSP-ответа действителен;
- Ключ электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении ExtendedKeyUsage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);

Адрес обращения к Службе актуальных статусов сертификатов Исполнителя размещается на официальном сайте Исполнителя.

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

- Подтверждена подлинность ЭП Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- Сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭП штампа времени действителен;
- Ключ электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;
- Сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) содержит в расширении ExtendedKeyUsage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);

Адрес обращения к Службе штампов времени Исполнителя размещается на официальном сайте Исполнителя.

8.9. Порядок оказания технической поддержки СЭП.

8.10.1. Исполнитель оказывает техническую поддержку СЭП на основании сертификата технической поддержки СЭП.

8.10.2. Сертификат технической поддержки СЭП выдается Уполномоченной организации при подключении Оператора СЭП. Сертификат технической поддержки СЭП должен быть зарегистрирован на портале технической поддержки Исполнителя по адресу: https://support.cryptopro.ru.

8.10.3. Исполнитель оказывает круглосуточную техническую поддержку СЭП через портал технической поддержки https://support.cryptopro.ru.

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

8.10.5. Обращение должно содержать следующую информацию:

- Тема сообщения с префиксом «SaaS. <Наименование Уполномоченной организации>»
- Дата и время (или диапазон времени) возникновения ошибки
- Интерфейс взаимодействия с СЭП (API или веб)

- Процесс, на котором возникает ошибка (регистрация пользователя, назначение аутентификации, получение/обновление/отзыв сертификата, подписание документа и т.п.)
- Логин пользователя в СЭП (опционально)
- Логин оператора в СЭП (опционально)
- Описание инцидента
- Возвращаемая ошибка со стороны СЭП
- Дополнительная информация при необходимости.

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

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

8.10.8. Время реакции на критические инциденты составляет 2 часа.

8.10.9. Время реакции на некритичные инциденты составляет 8 часов.

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

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

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

9.1. Форма 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», создается Удостоверяющим центром в соответствии с Порядком реализации функций Удостоверяющего центра.

9.2. Сроки действия ключей подписи и сертификатов ключей проверки электронной подписи устанавливаются Удостоверяющим центром в соответствии с Порядком реализации функций Удостоверяющего центра.

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

10. Дополнительные положения

10.1. Плановая и внеплановая смена ключей и сертификатов электронной подписи Удостоверяющего центра осуществляется в соответствии с Порядком реализации функций Удостоверяющего центра.

10.2. Нарушение конфиденциальности ключевых документов Оператора СЭП

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

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Оператор СЭП связывается с Исполнителем по телефону и приостанавливает действие сертификата ключа проверки электронной подписи, соответствующего ключу электронной подписи, конфиденциальность которого нарушена.

10.3. Конфиденциальность информации

10.3.1. Типы конфиденциальной информации

10.3.1.1. Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией. Исполнитель не осуществляет хранение ключей электронной подписи Операторов СЭП. Пользователи Удостоверяющего центра хранят свои ключи электронной подписи с использованием СЭП.

10.3.1.2. Персональная и корпоративная информация об Операторах СЭП и Пользователях Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной, в том числе информация об операциях, осуществляемых с использованием СЭП Исполнителем, и/или Уполномоченной организацией, и/или Пользователем Удостоверяющего центра.

10.3.1.3. 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.

10.3.1.4. Информация, содержащаяся в файле инициализации OTP-токенов, передаваемом Уполномоченной организацией Исполнителю считается конфиденциальной.

10.3.1.5. Ключи аутентификации в мобильном приложении СЭП, передаваемые Пользователям Удостоверяющего центра, считаются конфиденциальной информацией.

10.3.2. Типы информации, не являющейся конфиденциальной

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

10.3.2.2. Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов ключей проверки электронной подписи, не считается конфиденциальной.

10.3.2.3. Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, относятся к персональным данным, предоставление которых разрешено Оператором СЭП и Пользователем Удостоверяющего центра в целях надлежащего и своевременного получения услуг, связанных с выпуском квалифицированного сертификата ключа проверки электронной подписи.

10.4. Прекращение оказания услуг Исполнителя

10.4.1. В случае прекращения действия настоящего Регламента в отношении Уполномоченной организации действие сертификатов ключей проверки электронной подписи Оператора СЭП, как представителя Уполномоченной организации, а также действие сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, решение по выпуску

которых приняла Уполномоченная организация в лице Оператора СЭП, по усмотрению Исполнителя может быть прекращено. В этом случае от Сервиса электронной подписи отключаются все Сторонние центры идентификации и SMS-шлюз Уполномоченной Организации.

10.5. Непреодолимая сила (форс-мажор)

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

10.5.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

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

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

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

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

11. Список приложений

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

11.2. Приложение № 2. Форма доверенности Оператора СЭП.

11.3. Приложение № 3. Форма сертификата ключа проверки электронной подписи на бумажном носителе.

11.4. Приложение № 4. Форма заявления на подключение к Сервису электронной подписи Стороннего центра идентификации Уполномоченной Организации.

11.5. Приложение № 5. Форма заявления на подключение к Сервису электронной подписи SMS-шлюза Уполномоченной Организации.

11.6. Приложение № 6. Функции Сервиса электронной подписи.

11.7. Приложение № 7. Перечень параметров функционирования Сервиса электронной подписи для настройки доступа Операторов и Пользователей УЦ.

11.8. Приложение № 8. Форма заявления на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации.

11.9. Приложение № 9. Форма доверенности Оператора Стороннего центра идентификации Уполномоченной организации.

Приложение № 1
к Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на регистрацию Оператора СЭП)

Заявление на регистрацию Оператора СЭП

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

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

в лице_____,
(должность, фамилия, имя, отчество)

действующего на основании _____

Просит зарегистрировать в качестве Оператора СЭП:

_____
(фамилия, имя, отчество полномочного представителя – Оператора СЭП)

Со следующими идентификационными данными:

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

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

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

(указывается при необходимости такой рассылки)

Настоящим _____
(фамилия, имя, отчество Оператора СЭП,

_____ _____
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», а также на 5 (пять) лет после прекращения регистрации в Сервисе электронной подписи ООО «КРИПТО-ПРО». Настоящим также согласен с получением на вышеуказанный номер мобильного телефона и адрес электронной почты информационных сообщений, одноразовых паролей и уведомлений о выполняемых операциях с использованием выпущенного ключа электронной подписи.

Оператор СЭП _____

«____»_____ 20____г.

_____ _____/_____/

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

«_____»_____20____г.

М.П.

Приложение № 2
к Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма доверенности Оператора СЭП)

Доверенность

г._____ «_____»_____20___г.

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

в лице_____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество представителя)

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

действовать от имени _____
(полное наименование организации)

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

Настоящая доверенность действительна по «____»_____20____ г.

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

подтверждаю.

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

Приложение № 3к
Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма сертификата ключа проверки электронной
подписи на бумажном носителе)

Сертификат ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан:
ООО "Сочинские колбасы"
Версия: 3 (0x2)

Серийный номер: 61D0 B15A 0007 0000 007F
Издатель сертификата: CN = ООО «АУЦ», O = ООО "АУЦ", L = Москва, S = г. Москва, C = RU, E = ca@auc.ru, STREET = ул. Новая, д.1, ИНН = 007711111111, ОГРН = 1031111111111
Срок действия:
Действителен с: 01 сентября 2018 г. 14:14:00 UTC
Действителен по: 01 сентября 2019 г. 14:24:00 UTC
Владелец сертификата: SN = Петров, G = Пётр Петрович, T = Главный администратор, STREET = Курортный пр-т, дом 98/25, CN = ООО "Сочинские колбасы", OU = Отдел по закупкам оборудования, O = ООО "Сочинские колбасы", L = Сочи, S = 23 Краснодарский край, C = RU, E = petrov@sochikolb.ru, ИНН = 002311111111, ОГРН = 1234567890777
Ключ проверки электронной подписи:
Алгоритм ключа проверки электронной подписи:
Название: ГОСТ Р 34.10-2012 256 бит
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 76B0 EA28 93AF B020 70E5 869B E005 80A5 8EED 9157 67FD 5225 2657 2D04 F722 6217 3D98 F03E 8E31 D430 84F8 5E7E A79A 6411 E431 D408 8033 30A9 8629 B926 6CCC DD8D
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: e6 5f ca b6 c0 d0 38 a1 eb ab 96 4d 1a 44 21 f9 d9 6b 0b 09
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=a4 58 57 89 36 5a 85 01 b2 90 f9 9b 44 35 f6 42 b7 99 c4 6b Поставщик сертификата: Адрес каталога: CN CN = ООО «КРИПТО-ПРОАУЦ», O = ООО "КРИПТО-ПРОАУЦ", L = Москва, S = г. Москва, C = RU, E = qca@cryptoproauc.ru, STREET = ул. Сущёвский валНовая, д.16, стр.5, ИНН = 007717107991007711111111, ОГРН = 10377000854441031111111111 Серийный номер сертификата=07 a8 f5 9a 9a 64 15 95 46 5f 24 b0 3b 71 d4 53
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://q.cryptopro.ru/ra/cdp/A4585789365A8501B290F99B4435F642B799C46B.crl
6. Расширение 2.5.29.16
Название: Период использования закрытого ключа
Значение: Действителен с 01 сентября 2018 г. 18:14:00 Действителен по 01 сентября 2019 г. 18:14:00
7. Расширение 1.2.643.100.111
Название: Средство электронной подписи владельца
Значение: Средство электронной подписи: СКЗИ «КриптоПро CSP» версии 5.0 R2 КС1 исполнение 1-Base
8. Расширение 1.2.643.100.112
Название: Средства электронной подписи и УЦ издателя
Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP" (версия 4.0) Заключение на средство ЭП: Сертификат соответствия СФ/124-3010 от 30.12.2016 Средство УЦ: ПАК "КриптоПро УЦ" (версии 2.0) Заключение на средство УЦ: Сертификат соответствия № СФ/128-2983 от 18.11.2016
9. Расширение 2.5.29.32
Название: Политики сертификата
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11-2012/34.10-2012 256 бит
Идентификатор: 1.2.643.2.2.3
Значение: 0D47 F9D8 F0EE B4FE F915 5356 DECF F1CE 1275 A4E9 5973 1D99 F177 2453 DE0E 8DA5 1F86 B62C 024D 21F0 738F 604E 1774 DB30 91C5 B52B D14B 1727 8979 C98D 94B3 C9B9

Подпись владельца сертификата/полномочного представителя:_____/_____

«_____»_____20____г.

Приложение № 4
к Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(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 ЦИ 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 № 5
к Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на подключение SMS-шлюза)

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

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

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

в лице_____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

К настоящему заявлению прилагаются в электронной форме:

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

_____ _____/_____/

«____»_____20_____г.

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

«_____»_____ 20__ г.

М.П.

Приложение № 6
к Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Функции Сервиса электронной подписи)

Реализуемые функции Сервиса электронной подписи ООО «КРИПТО-ПРО»

1. Назначение сервиса

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

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

2. Поддерживаемые форматы и стандарты

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

Поддерживаемые форматы криптографических сообщений:

1. «Чистая» (необработанная) 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 и CAdES-X Long Type 1);
3. Подпись XML-документов (XML Digital Signature, XMLDSig);
4. Подпись документов PDF (Open Document Format);
5. Подпись документов Microsoft Office (Office Open XML).

3. Используемые средства электронной подписи

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

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

4. Предоставление доступа к сервису

Доступ к Сервису электронной подписи осуществляется круглосуточно в режиме 24x7 по каналам связи посредством Веб-интерфейса, предоставляемого Удостоверяющим центром, или Прикладного интерфейса, используемого для подключения Информационных систем Уполномоченной организации в соответствии руководством разработчика программного обеспечения 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 ключа аутентификации в мобильном приложении СЭП на устройствах Пользователей УЦ; одноразового кода, высылаемого Пользователям УЦ в информационном сообщении или формируемого с помощью OTP-токена.

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

5. Информирование Пользователей Удостоверяющего центра

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

6. Защита информации

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

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

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

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

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

7. Правила пользования Сервисом электронной подписи

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

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

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

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

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

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

8. Аудит Сервиса электронной подписи

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

Приложение № 7
к Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма перечня параметров функционирования СЭП для настройки доступа Операторов и Пользователей УЦ)

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

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.	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><th colspan="5">Настройки СЭП</th></tr>
<tr><td rowspan="3">4.</td><td rowspan="3">Использование PIN-кода для ключевого контейнера</td><td colspan="3">Выбрать из списка (одно):</td></tr>
<tr><td></td><td colspan="2">Обязательно</td></tr>
<tr><td></td><td colspan="2">Запрещено</td></tr>
<tr><td></td><td></td><td>+</td><td colspan="2">Опционально (позволять задавать)</td></tr>
<tr><th colspan="5">Профиль Пользователя</th></tr>
<tr><td rowspan="16">5.</td><td rowspan="16">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>
<tr><td rowspan="3">6.</td><td rowspan="3">Самостоятельное редактирование профиля Пользователем</td><td colspan="3">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td colspan="2">Запретить</td></tr>
<tr><td></td><td colspan="2">Разрешить</td></tr>
<tr><th colspan="5">Политика учетных записей Пользователей</th></tr>
<tr><td rowspan="3">7.</td><td rowspan="3">Используемые идентификаторы Пользователя[4]</td><td colspan="3">Выбрать из списка ниже (одно, или несколько):</td></tr>
<tr><td>+</td><td colspan="2">Логин</td></tr>
<tr><td></td><td colspan="2">Номер телефона</td></tr>
</table>

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

			Адрес электронной почты (e-mail)
8.	Подтверждение номера телефона Пользователя отправкой SMS	*Выбрать из списка (одно):*	
		+	Не требуется
			Требуется
9.	Подтверждение e-mail Пользователя отправкой электронного письма	*Выбрать из списка (одно):*	
		+	Не требуется
			Требуется
10.	Самостоятельная регистрация Пользователей в СЭП	*Выбрать из списка (одно):*	
		+	Запрещена
			Разрешена
11.	Временная блокировка самостоятельно зарегистрировавшихся Пользователей в СЭП[5]	*Выбрать из списка (одно):*	
		+	Нет
			Да
12.	Список операций, разрешенных для Пользователя	*Выбрать из списка ниже (одно, или несколько):*	
		+	Подпись документа
		+	Шифрование/расшифрование документа
			Создание запроса на сертификат
			Удаление сертификата
		+	Смена PIN-кода для доступа к закрытому ключу сертификата
13.	Предоставить Оператору возможность управления списком разрешенных операций	*Выбрать из списка (одно):*	
			Нет
		+	Да
14.	Предоставить Пользователю возможность управления списком разрешенных операций	*Выбрать из списка (одно):*	
		+	Нет
			Да

[5] Заполняется только если самостоятельная регистрация Пользователей в СЭП разрешена (п. 11).

Настройки первичной аутентификации Пользователей			
15.	Методы первичной аутентификации Пользователей	*Выбрать из списка ниже (одно):*	
			Только идентификация[6]
		+	По паролю
16.	Разрешить Пользователям самостоятельное изменение настроек первичной аутентификации[7]	*Выбрать из списка (одно):*	
		+	Нет
			Да
Политики долговременных паролей			
17.	Длина долговременных паролей (*от 1 до 256 символов*)	8 символов	
18.	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[8]
19.	Максимальное количество попыток ввода долговременного пароля до блокирования учётной записи	*Выбрать из списка (одно):*	
		+	5 (можно указать собственное значение)
			0 (Блокирование отключено)
20.	Срок действия долговременного пароля (*в днях*)	*Выбрать из списка (одно):*	
		+	Срок действия не ограничен
			Указать количество дней
21.	Требовать смену пароля Пользователя при первом входе в СЭП[9]	*Выбрать из списка (одно):*	
		+	Не требовать
			Требовать

[6] Требуется использование вторичного фактора аутентификации (мобильное приложение или одноразовый пароль – п.22).

[7] Требуется использование вторичного фактора аутентификации (мобильное приложение или одноразовый пароль – п.22).

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

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

Политики вторичной аутентификации			
22.	Альтернативные методы вторичной аутентификации Пользователей[10]	*Выбрать из списка (одно):*	
			Одноразовый пароль по SMS
			Одноразовый пароль по EMAIL
			Генератор одноразовых паролей[11]
23.	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
		+	Расшифрование или аутентификация с помощью Cloud CSP
		+	Выпуск маркера безопасности («вход» Пользователя)[12]
24.	Разрешить Пользователям самостоятельное изменение настроек вторичной аутентификации[13]	*Выбрать из списка (одно):*	
		+	Нет
			Да
25.	Предоставить Оператору возможность управления списком операций, требующих подтверждения[14]	*Выбрать из списка (одно):*	
			Нет
		+	Да

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

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

[12] Если в методах первичной аутентификации Пользователей (п. 15) 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.

[13] Не рекомендуется разрешать Пользователям самостоятельно изменять настройки вторичной аутентификации, если в качестве метода первичной аутентификации выбрана только идентификация (п. 15), т.к. в результате может возникнуть небезопасная конфигурация аутентификации.

[14] Не рекомендуется разрешать Оператору самостоятельно изменять настройки вторичной аутентификации, если в качестве метода первичной аутентификации Пользователей выбрана только идентификация (п. 15), т.к. в результате может возникнуть небезопасная конфигурация аутентификации.

26.	Предоставить Пользователю возможность управления списком операций, требующих подтверждения	*Выбрать из списка (одно):*	
		+	Нет
			Да
Настройки для мобильного приложения			
27.	Максимальное время хранения документов (до 7 дней)	3 дня	
28.	Срок действия QR-кода для инициализации мобильного устройства	7 дней	
29.	Список операций, разрешенных для выполнения из мобильного приложения	*Выбрать из списка (одно, или несколько):*	
		+	Подпись документа
			Создание запроса на сертификат
Политики одноразовых паролей и паролей мобильных приложений			
30.	Длина одноразовых паролей (*от 1 до 256 символов*)	6 символов	
31.	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
32.	Максимальное количество попыток ввода одноразового пароля до блокирования учётной записи	*Выбрать из списка (одно):*	
		+	3 (можно указать собственное значение)
			Блокирование отключено
33.	Отправка кодов активации для QR-кодов мобильных приложений[15]	*Выбрать из списка (одно):*	
		+	Требуется
			Не требуется

[15] Отправлять код активации по SMS или E-mail.

<table>
<tr><td rowspan="5">34.</td><td rowspan="5">Сложность паролей для мобильных приложений</td><td colspan="2">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td>Без пароля/любой пароль</td></tr>
<tr><td></td><td>Минимум 6 символов</td></tr>
<tr><td></td><td>Минимум 8 символов, буквы в разном регистре</td></tr>
<tr><td></td><td>Минимум 8 символов, цифры и буквы в разном регистре</td></tr>
<tr><td colspan="4">Политики операций[16]</td></tr>
<tr><td>35.</td><td>Время жизни операции в секундах[17]</td><td colspan="2">300 (можно указать собственное значение, но не более 3 суток)</td></tr>
<tr><td colspan="4">Параметры OAuth</td></tr>
<tr><td rowspan="3">36.</td><td rowspan="3">Адрес перенаправления redirect_uri[18]</td><td colspan="2">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td>Значение по умолчанию</td></tr>
<tr><td></td><td>(указать адрес перенаправления)</td></tr>
<tr><td colspan="4">Группы Пользователей СЭП</td></tr>
<tr><td rowspan="4">37.</td><td rowspan="4">Информация о группах пользователей и их Операторах</td><td colspan="2">Выбрать из списка (одно):</td></tr>
<tr><td>+</td><td>Группа пользователей по умолчанию</td></tr>
<tr><td rowspan="2"></td><td>Собственные группы пользователей (указать в таблице ниже)</td></tr>
<tr><td>
<table>
<tr><td>Имя группы</td><td>Описание группы</td><td>Логин Оператора группы</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td colspan="4">Настройки уведомлений</td></tr>
<tr><td>38.</td><td>Перечень событий для рассылки уведомлений Пользователям и Операторам по электронной почте (email)[19]</td><td colspan="2">Выбрать значения уведомлений Операторов и Пользователей СЭП во вложенной таблице (вкладка NEW):
Оповещения_СЭП 2021_08.xlsx</td></tr>
<tr><td rowspan="6">39.</td><td rowspan="6">Перечень адресов электронной почты (email) для рассылки уведомлений Операторам о событиях СЭП</td><td colspan="2">Указать адреса электронной почты (e-mail) Операторов СЭП:</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
</table>

[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.

Другие настройки		
40.	Другие настройки[20]	

_____ _____ /_____/
(ФИО Оператора) (подпись) (фамилия, инициалы)
«___»_____20__ г.

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

[20] Заполняется по согласованию.

Приложение № 8
Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на регистрацию Оператора Стороннего центра идентификации)

Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации

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

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

в лице_____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

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

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

(указывается при необходимости такой рассылки)

Настоящим _____
(фамилия, имя, отчество Оператора СЦИ)

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

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

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

_____ _____/_____/
«____»_____ 20_____г.

_____ _____/_____/
(Должность руководителя организации) (подпись) (фамилия, инициалы)
«____»_____ 20_____г.
М.П.

Приложение № 9
Регламенту по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма доверенности Оператора Стороннего центра идентификации)

Доверенность

г._____ «_____»_____20___г.

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

в лице_____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

действовать от имени _____
(полное наименование организации)

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

Настоящая доверенность действительна по «____»_____ 20___г.

Подпись Оператора Стороннего центра идентификации подтверждаю.

_____

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