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

РЕГЛАМЕНТ

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

Редакция № 1

г. Москва
2015

1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дельнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва (Свидетельство о регистрации № 001.602.749 выдано 16.11.1999 г. Государственным учреждением Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003 г.).

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании Свидетельства об аккредитации удостоверяющего центра № 26 от 06 августа 2012 г., выданного Минкомсвязи России (Федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи), и на основании следующих лицензий, опубликованных в сети Интернет по адресу: https://www.cryptopro.ru/about/licenses.

Реквизиты ООО «КРИПТО-ПРО»:

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

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

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

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

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

ИНН/КПП: 7717107991/771901001

ОГРН: 1037700085444

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

Код по ОКПО: 51282566

Контактные телефоны, факс, адрес электронной почты:

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

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

2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Договором, а также термины и определения их дополняющие и конкретизирующие, а именно:

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

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

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

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

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

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

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

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

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

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра, либо подписанный Оператором Удостоверяющего центра и заверенный печатью Уполномоченной организации. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

Многофакторная аутентификация - процедура проверки подлинности Пользователя Удостоверяющего центра при осуществлении доступа с использованием двух и более уникальных характеристик, известных или присущих только Пользователю Удостоверяющего центра (факторов аутентификации). При управлении доступом к Сервису электронной подписи для первичной аутентификации Пользователя Удостоверяющего Центра используется постоянно действующий пароль, самостоятельно определяемый Пользователем Удостоверяющего центра, для вторичной аутентификации – одноразовый пароль, формируемый Сервисом электронной подписи и высылаемый Пользователю Удостоверяющего центра в информационном сообщении на номер мобильного телефона, указанный Пользователем Удостоверяющего центра при регистрации, или OTP-токеном, выдаваемый Оператором УЦ по заявлению Пользователя Удостоверяющего центра.. Уполномоченная организация вправе использовать дополнительные факторы аутентификации для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи совместно с собственным Сторонним центром идентификации.

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

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

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

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

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем 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. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи.

Прикладной интерфейс, предоставляемый Удостоверяющим центром (API) – интерфейс подключения Информационных систем Уполномоченной организации к Удостоверяющему центру по линиям связи для получения доступа к функциям электронной подписи, управления сертификатами ключей проверки электронной подписи, реализованный по протоколу SOAP в соответствии с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика» и защищенный с использованием средств криптографической защиты информации, совместимых со средствами Удостоверяющего центра.

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

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

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

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

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

Сертификат ключа проверки электронной подписи - электронный документ, выданный Удостоверяющим центром или доверенным лицом Удостоверяющего центра 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) если:

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

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

Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра (Сертификат Пользователя УЦ) - сертификат ключа проверки электронной подписи,

соответствующий которому ключ электронной подписи создан и хранится с использованием СЭП.

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

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

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

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

Список отозванных сертификатов (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 Регламента, используемое для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и (или) ключа проверки электронной подписи.

Сторонний центр идентификации – система аутентификации Уполномоченной организации, подключаемая к Сервису электронной подписи по протоколу SAML 2.0 в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» и используемая Уполномоченной организацией для управления доступом Пользователей Удостоверяющего центра к Сервису электронной подписи.

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

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

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

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

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

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

Cryptographic Message Syntax (CMS) – стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом RFC 4490 «Using the GOST 28147-89, GOSTR 34.11-94, GOSTR 34.10-94, and GOSTR 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

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

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

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

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

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

SMS-шлюз – служба рассылки информационных сообщений Уполномоченной Организации, подключаемая к Сервису электронной подписи в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» и используемая Уполномоченной организацией для отправки Пользователям Удостоверяющего центра одноразовых паролей и уведомлений о выполняемых в СЭП операциях.

3. Общие положения

3.1. Предмет Регламента

3.1.1. Регламент Удостоверяющего центра ООО «КРИПТО-ПРО» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи (Схема обслуживания: распределенная с оператором СЭП), именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

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

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

3.2. Применение Регламента

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

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

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

3.3. Изменение Регламента

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

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

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

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

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

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

4. Предоставление информации

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

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

4.3. Удостоверяющий центр предоставляет Стороне, присоединившейся к Регламенту по ее требованию:

4.3.1. Копию лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), выданную Удостоверяющему центру.

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

- выписку или нотариально заверенную копию выписки из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента запроса Удостоверяющего центра;
- нотариально заверенные копии учредительных документов Уполномоченной организации;
- нотариально заверенную копию свидетельства о внесении записи о юридическом лице в Единый государственный реестр юридических лиц;
- нотариально заверенную копию свидетельства о постановке на учет в налоговом органе;
- документы, подтверждающие финансовое обеспечение своей ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи и идентифицирующей владельца сертификата ключа проверки электронной подписи;
- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность - для Оператора Удостоверяющего центр (либо нотариально заверенные копии этих документов);
- иные документы, установленные Регламентом Удостоверяющего центра, а также дополнительные документы по усмотрению Удостоверяющего центра.

4.5. Присоединяясь к настоящему Регламенту, Уполномоченная организация в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» поручает Удостоверяющему центру в лице их уполномоченных работников и иных лиц, привлекаемых Удостоверяющим центром, совершать с персональными данными, содержащимися в

документах, представленных Уполномоченной организацией Удостоверяющему центру для присоединения к настоящему Регламенту, а также в документах, которые будут представлены Уполномоченной организацией Удостоверяющему центру в соответствии с Регламентом, следующие действия (с использованием и без использования средств автоматизации): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), в том числе передача уполномоченным работникам Удостоверяющего центра, обезличивание, блокирование, удаление, уничтожение персональных данных (далее – «обработка») в целях принятия Удостоверяющим центром решения о возможности присоединения Уполномоченной организации к Регламенту, доступа к СЭП, в целях исполнения Регламента, реализации вытекающих из Регламента прав и обязанностей, а также в целях осуществления Удостоверяющим центром функций, возложенных законодательством Российской Федерации.

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

Уполномоченная организация поручает Удостоверяющему центру в лице указанных выше работников и иных лиц, ими привлекаемых, осуществлять обработку персональных данных с соблюдением принципов и правил обработки персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», и обеспечением безопасности персональных данных при их обработке, на безвозмездной основе.

Уполномоченная организация подтверждает, что им получено письменное согласие субъектов персональных данных, чьи персональные данные содержатся в представленных Уполномоченной организацией Удостоверяющему центру документах, на обработку Удостоверяющим центром этих персональных данных по поручению Уполномоченной организации в указанных выше целях, а также гарантирует, что содержащие персональные данные документы будут представляться Уполномоченной организацией Удостоверяющему центру в соответствии с Регламентом с согласия субъектов персональных данных, чьи персональные данные содержатся в таких документах. Уполномоченная организация несет все неблагоприятные последствия, связанные с неполучением Уполномоченной организацией таких согласий.

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

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

5. Права и обязанности сторон

5.1. Удостоверяющий центр обязан:

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

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

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

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

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

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

5.1.7. Создать сертификат ключа проверки электронной подписи Оператора Удостоверяющего центра по заявлению на создание сертификата в соответствии с порядком, определенным в настоящем Регламенте.

5.1.8. Предоставить аутентифицированным Пользователям Удостоверяющего центра, получившим сертификат ключа проверки электронной подписи, доступ к СЭП и обеспечить круглосуточное функционирование СЭП в режиме 24x7 в соответствии с настоящим Регламентом. Восстановить функционирование СЭП в течение 1 (одного) часа рабочего времени в случае проведения плановых регламентных работ или возникновения внештатных ситуаций. Доступные Пользователям функциональные возможности СЭП приведены в Приложении № 17.

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

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

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

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

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

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

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

5.1.16. Прекратить действие сертификатов ключей проверки электронной подписи Оператора и Пользователя Удостоверяющего центра в случае нарушения конфиденциальности ключа

электронной подписи Удостоверяющего центра, с использованием которого были созданы сертификаты ключей проверки электронной подписи Операторов и Пользователей Удостоверяющего центра.

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

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

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

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

5.1.21. Предоставить Уполномоченной организации необходимые права для:

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

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

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

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

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

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

5.1.22. Зарегистрировать в СЭП Оператора подключенного Стороннего центра идентификации Уполномоченной организации в соответствии с заявлением по форме Приложения 19, полученного от Уполномоченной организации.

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

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

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

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

5.2. Уполномоченная организация обязана:

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

5.2.2. Известить Удостоверяющий центр об изменениях реквизитов Уполномоченной организации и по требованию Удостоверяющего Центра предоставить соответствующие подтверждающие документы, указанные в п.4.4 настоящего Регламента, в течение 5 (пяти) рабочих дней с момента регистрации изменений.

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

5.2.4. После проведения проверки с использованием тестовых сертификатов согласовать и подписать предоставленный Удостоверяющим центром перечень настроенных параметров функционирования СЭП для доступа Операторов и Пользователей УЦ по форме в соответствии с Приложением 18.

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

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

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

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

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

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

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

5.2.10.2. Обеспечить конфиденциальность ключей электронных подписей.

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

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

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

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

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

5.2.10.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

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

5.2.10.10. Для создания и проверки усиленных квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи использовать СЭП и сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

5.3. Удостоверяющий центр имеет право:

5.3.1. Отказать в создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае ненадлежащего оформления заявления на создание сертификата ключа проверки электронной подписи.

5.3.2. Отказать в создании сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра в случае не предоставления и/или ненадлежащего предоставления документов, установленных п. 4.4 настоящего Регламента.

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

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

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

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

5.3.7. Отказать в создании и управлении сертификатами ключей проверки электронной подписи по заявкам Оператора УЦ до получения от Уполномоченной организации подписанного перечня параметров функционирования СЭП для настройки прав доступа Операторов и Пользователей УЦ по форме в соответствии с Приложением № 13.

5.3.8. Отказать в подключении Стороннего центра идентификации Уполномоченной организации в случае ненадлежащего оформления заявления на подключение Стороннего центра идентификации в соответствии с Приложением 15.

5.3.9. Отказать в подключении SMS-шлюза Уполномоченной организации в случае ненадлежащего оформления заявления на подключение SMS-шлюза в соответствии с Приложением 16.

5.3.10. Отказать в регистрации Оператора Стороннего центра идентификации до получения надлежащим образом (в соответствии с Приложением 15) оформленного заявления на подключение Стороннего центра идентификации Уполномоченной организации или в случае ненадлежащего оформления заявления на регистрацию Оператора СЦИ в соответствии с Приложением 19.

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

5.4. Уполномоченная организация имеет право:

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

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

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

5.4.4. Подать в Удостоверяющий центр заявление по форме в соответствии с Приложением 19 на регистрацию в СЭП Оператора Стороннего центра идентификации Уполномоченной организации.

5.4.5. Осуществить в соответствии с п.8.8 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.

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

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

5.4.8. Делегировать Пользователям УЦ право подачи заявки в УЦ на создание и управление своими сертификатами ключей проверки электронной подписи посредством Веб- или Прикладного интерфейса СЭП, предоставляемых Удостоверяющим центром. Предоставленные Уполномоченной организацией права Пользователей УЦ определяются параметрами функционирования СЭП в соответствии с Приложением 18 и Регламентом деятельности Уполномоченной организации. Уполномоченная организация несет всю полноту своих обязанностей и ответственности за создаваемые Удостоверяющим центром сертификаты по заявкам Пользователей УЦ в соответствии с предоставленными им Уполномоченной организацией правами.

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

5.4.10. Оператор Удостоверяющего центра имеет право:

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

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

5.4.10.3. Принимать решения о создании и выдаче сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра.

5.4.10.4. Прекращать, приостанавливать и возобновлять действие сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра, решение по созданию которых было принято Оператором Удостоверяющего центра.

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

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

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

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

6. Ответственность сторон

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

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

6.3. Удостоверяющий центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях Оператора Удостоверяющего центра.

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

6.5. Вся ответственность по занесению данных в сертификаты ключей проверки электронной подписи Пользователей Удостоверяющего центра, принятию решений по созданию, выдаче и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, формированию копий сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра полностью возлагается на Уполномоченную организацию.

6.6. Вся ответственность по достоверной аутентификации и управлению доступом Пользователей Удостоверяющего центра к Сервису электронной подписи при использовании стороннего центра идентификации и (или) SMS-шлюза полностью возлагается на Уполномоченную организацию.

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

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

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

7. Разрешение споров

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

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

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

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

8. Порядок предоставления и пользования услугами Удостоверяющего Центра

8.1. Общий порядок пользования услугами Удостоверяющего центра

Уполномоченная организация в лице Оператора Удостоверяющего центра осуществляет формирование ключей электронной подписи, принятие решений по созданию, выдаче и управлению сертификатами ключей проверки электронной подписи с использованием СЭП.

Удостоверяющий центр осуществляет действия по созданию и управлению сертификатами ключей проверки электронной подписи, решение по которым принимает Оператор Удостоверяющего центра, на основании электронных заявлений, формируемых в СЭП по команде Оператора Удостоверяющего центра.

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

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

8.2. Создание сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра

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

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

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

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

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

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

Создание и выдача сертификатов ключей проверки электронной подписи Оператору Удостоверяющего центра осуществляется Удостоверяющим центром в день прибытия заявителя. День прибытия заявителя согласовывается с Администратором Удостоверяющего

центра. Удостоверяющий центр вправе отказать в создании сертификатов по заявлениям, поступившим в Удостоверяющим центр без согласования дня прибытия заявителя.

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

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

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

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

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

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

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

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

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

Подача заявления в Удостоверяющий центр на прекращение действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 4 настоящего Регламента.

После получения Удостоверяющим центром заявления на прекращение действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра

осуществляет его рассмотрение и обработку. Обработка заявления на прекращение действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Заявка подается в Удостоверяющий центр по телефону.

Оператор Удостоверяющего центра должен сообщить Администратору Удостоверяющего центра следующую информацию:

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

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

После принятия заявки Администратор Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа проверки электронной подписи, которое должно быть осуществлено в течение рабочего дня поступления данной заявки.

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

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

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

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

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

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

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

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра только по заявлению его владельца

и только в том случае, если действие сертификата ключа проверки электронной подписи было приостановлено.

Подача заявления в Удостоверяющий центр на возобновление действия сертификата ключа проверки электронной подписи Оператора Удостоверяющего центра может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 6 настоящего Регламента.

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

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

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

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

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

8.6. Подключение Информационной системы Уполномоченной Организации к Сервису электронной подписи

Удостоверяющий центр предоставляет Уполномоченной организации Прикладной интерфейс подключения к Сервису электронной подписи в соответствии с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика». Защита передаваемых от Информационной системы к Сервису электронной подписи данных осуществляется в соответствии с требованиями Уполномоченной Организации с использованием СКЗИ, совместимых со средствами Удостоверяющего центра.

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

Подключение Стороннего центра идентификации Уполномоченной организации к Сервису электронной подписи осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению от Уполномоченной Организации по форме в соответствии с Приложение № 10. Заявление передается в Удостоверяющий центр курьерской или почтовой связью. Вместе с заявлением на носителе информации передается сертификат, используемый для проверки подписи SAML-токенов, передаваемых от Стороннего центра идентификации.

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

При смене Уполномоченной организацией сертификата Стороннего центра идентификации осуществляется повторное подключение Стороннего центра идентификации в соответствии с п.8.7 настоящего Регламента.

Заявление на подключение и сертификат Стороннего центра идентификации могут быть отправлены Администратору Удостоверяющего центра в электронной форме, подписанные электронной подписью Оператора УЦ и руководителя Уполномоченной организации с использованием сертификатов, созданных Удостоверяющим центром.

Регистрацию Оператора СЦИ в СЭП выполняет Удостоверяющий центр после получения заявления по форме в соответствии с Приложением 14. Заявление передается в Удостоверяющий центр курьерской или почтовой связью.

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

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

Подключение SMS-шлюза Уполномоченной Организации к Сервису электронной подписи осуществляется в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора» по заявлению от Уполномоченной Организации по форме в соответствии с Приложение № 12. Заявление передается в Удостоверяющий центр курьерской или почтовой связью.

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

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

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

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

Получение документированной информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется на основании заявления, направляемого Оператором Удостоверяющего центра. Данное заявление оформляется по форме Приложения №7 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

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

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

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

8.10. Подтверждение подлинности электронной подписи в электронном документе

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

По запросу Уполномоченной Организации, Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению электронной подписи в электронном документе, созданной с использованием Сервиса электронной подписи.

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

В данном случае для подтверждения подлинности ЭП в электронных документах Оператор удостоверяющего центра подает заявление в Удостоверяющий центр по форме, приведенной в Приложении №8.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

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

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

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

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

Заключение содержит:

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

Отчет по выполненной проверке содержит:

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

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

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

В том случае, если ЭП сформирована без использования Сервиса электронной подписи, то проведение экспертных работ по подтверждению подлинности ЭП осуществляется в рамках заключения отдельного договора (соглашения) между Удостоверяющим центром

Уполномоченной Организацией. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором (соглашением).

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

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

Удостоверяющий центр выполняет действия по созданию сертификатов ключей проверки электронной подписи Пользователя УЦ, прекращению действия сертификатов ключей проверки электронной подписи Пользователя УЦ, приостановлению и возобновлению действий сертификатов ключей проверки электронной подписи Пользователя УЦ в соответствии с настройками параметров функционирования СЭП, определенных по форме Приложения №13, на основании заявок в электронной форме внутреннего формата СЭП, направляемых Оператором Удостоверяющего центра и (или) Пользователями Удостоверяющего центра с использованием Веб- или Прикладного интерфейса СЭП, предоставляемого Удостоверяющим центром. Выполнение указанных действий осуществляется Удостоверяющим центром при соответствии параметров аутентификации заявителя регистрационным данным:

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

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

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

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

Владелец сертификата ключа проверки электронной подписи Пользователя УЦ подтверждает использование своего ключа электронной подписи посредством ввода индивидуального ПИН-кода доступа к ключу электронной подписи и одноразового пароля, формируемого СЭП и отправляемого в информационном сообщении на номер мобильного телефона владельца сертификата, указанный при регистрации Пользователя Удостоверяющего центра. Одноразовый пароль для подтверждения операций с ключом электронной подписи

может быть сформирован OTP-токеном, выдаваемым владельцу соответствующего сертификата ключа проверки электронной подписи Оператором УЦ по заявлению Пользователя Удостоверяющего центра.

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

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

- Подтверждена подлинность ЭП Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;
- Сертификат ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности ЭП OCSP-ответа действителен;
- Ключ электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении ExtendedKeyUsage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);
- Сертификат ключа проверки электронной подписи, статус которого установлен с использованием данного OCSP-ответа, издан Удостоверяющим центром и содержит в расширении ExtendedKeyUsage или ApplicationPolicy область использования - Пользователь службы актуальных статусов (1.2.643.2.2.34.26).

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра–http://ocsp.cryptopro.ru/ocsp/ocsp.srf. Указанный адрес заносится в расширение AuthorityInformationAccess (AIA) издаваемых Удостоверяющим центров сертификатов ключей проверки электронной подписей.

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

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

ApplicationPolicy область использования - Пользователь службы штампов времени (1.2.643.2.2.34.25).

Адрес обращения к Службе штампов времени Удостоверяющего центра– http://tsp.cryptopro.ru/tsp/tsp.srf.

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

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

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

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

- в поле Subject (идентифицирует владельца сертификата):
  - Поле E (Email) – адрес электронной почты;
  - Поле T (Title) – должность полномочного представителя юридического лица, данные которого занесены в сертификат наряду с наименованием юридического лица (если владелец сертификата – юридическое лицо);
- расширение Private Key Validity Period – срок действия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи, следующего формата:
  Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;
  Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;
- расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) – набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с сертификатом ключа проверки электронной подписи (если такие ограничения установлены);
- расширение CRL Distribution Point (Точка распространения списка отозванных сертификатов) - набор адресов точек распространения списков отозванных сертификатов;
- расширение Authority Information Access (Доступ к информации о центре) – Адрес обращения к Службе актуальных статусов сертификатов, Адрес размещения сертификата Удостоверяющего центра;
- иные поля и расширения по усмотрению Удостоверяющего центра.

9.2. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (ResonCode) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001

Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата ключа проверки электронной подписи (корневого сертификата) Удостоверяющего Центра

9.3. Сроки действия ключевых документов

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

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

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

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

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

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

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

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

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

9.3.2. Сроки действия ключевых документов Оператора и Пользователя Удостоверяющего центра

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

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

Срок действия сертификата ключа проверки электронной подписи Оператора и Пользователя Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Оператора и Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

10. Дополнительные положения

10.1. Плановая смена ключей электронной подписи Удостоверяющего Центра

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

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

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

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

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

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

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

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

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

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

10.3. Нарушение конфиденциальности ключевых документов Оператора Удостоверяющего центра

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

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Оператор связывается с Удостоверяющим центром по телефону и приостанавливает действие сертификата, соответствующего ключу, конфиденциальность которого нарушена, посредством подачи заявления на приостановление действие сертификата в устной форме (пункт 8.4.2 настоящего Регламента).

Оператор Удостоверяющего центра осуществляет выдачу сертификата ключа проверки электронной подписи Оператору УЦ в соответствии с пунктом 8.2 настоящего Регламента.

10.4. Конфиденциальность информации

10.4.1. Типы конфиденциальной информации

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

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

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

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

10.4.2. Типы информации, не являющейся конфиденциальной

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

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

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

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

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

10.4.3. Исключительные полномочия Удостоверяющего центра

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

10.5. Хранение сертификатов ключей проверки электронной подписи в Удостоверяющем центре

Срок хранения сертификата ключа проверки электронной подписи в Удостоверяющем центре осуществляется в течение всего периода его действия и 5 (пяти) лет после

прекращения его действия. По истечении указанного срока хранения сертификаты ключа проверки электронной подписи переводятся в режим архивного хранения.

10.6. Прекращение оказания услуг Удостоверяющим центром

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

10.7. Непреодолимая сила (форс-мажор)

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

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

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

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

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

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

11. Список приложений

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

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

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

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

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

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

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

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

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

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

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

11.12. Приложение №12. Функции Сервиса электронной подписи

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

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

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

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

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

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

действующего на основании _____

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

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

_____
(фамилия, имя, отчество полномочного представителя)

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

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

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

соглашается с обработкой своих персональных данных ООО «КРИПТО-ПРО» и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, относятся к общедоступным персональным данным.

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

_____

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

(указывается при необходимости такой рассылки)

Оператор Удостоверяющего центра
ООО «КРИПТО-ПРО» _____

«____» _____ 20____ г.

_____ _____ /_____/

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

«___»_____20__ г.

М.П.

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

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

Доверенность

г. _____ «_____» _____20___ г.

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

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

действовать от имени _____
(полное наименование организации)

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

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

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

подтверждаю.

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

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

Доверенность

г. _____ «_____» _____20___ г.

_____
(полное наименование 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)

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

_____
(фамилия, имя, отчество Пользователя Удостоверяющего центра)

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

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

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

подтверждаю.

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

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

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

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

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

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

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

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

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

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

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

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

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

Срок приостановления действия сертификата _____ дней.
(количество прописью)

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

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

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

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

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

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

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

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

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

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

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

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

Заявление на подтверждение подлинности электронной подписи в электронном документе

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

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

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

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

«____» _____ 20____ г.

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

«___»_____20__ г.

М.П.

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

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

Копия сертификата ключа проверки электронной подписи

Сведения о сертификате:
Кому выдан:
ООО "Сочинские колбасы"
Версия: 3 (0x2)
Серийный номер: 61D0 B15A 0007 0000 007F
Издатель сертификата: CN = ООО «КРИПТО-ПРО», O = ООО "КРИПТО-ПРО", L = Москва, S = г. Москва, C = RU, E = qca@cryptopro.ru, STREET = ул. Сущёвский вал, д.16, стр.5, ИНН = 007717107991, ОГРН = 1037700085444
Срок действия:
Действителен с: 01 сентября 2012 г. 14:14:00 UTC
Действителен по: 01 сентября 2013 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 34.10-2001
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 (f0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: e6 5f ca b6 c0 d0 38 a1 eb ab 96 4d 1a 44 21 f9 d9 6b 0b 09
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=a4 58 57 89 36 5a 85 01 b2 90 f9 9b 44 35 f6 42 b7 99 c4 6b Поставщик сертификата: Адрес каталога: CN = ООО «КРИПТО-ПРО», O = ООО "КРИПТО-ПРО", L = Москва, S = г. Москва, C = RU, E = qca@cryptopro.ru, STREET = ул. Сущёвский вал, д.16, стр.5, ИНН = 007717107991, ОГРН = 1037700085444 Серийный номер сертификата=07 a8 f5 9a 9a 64 15 95 46 5f 24 b0 3b 71 d4 53
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://q.cryptopro.ru/ra/cdp/A4585789365A8501B290F99B4435F642B799C46B.crl
6. Расширение 2.5.29.16
Название: Период использования закрытого ключа
Значение: Действителен с 01 сентября 2012 г. 18:14:00 Действителен по 01 сентября 2013 г. 18:14:00
7. Расширение 1.2.643.100.111
Название: Средство электронной подписи владельца
Значение: Средство электронной подписи: КриптоПро CSP (версия 3.6)
8. Расширение 1.2.643.100.112
Название: Средства электронной подписи и УЦ издателя
Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6) Заключение на средство ЭП: Сертификат соответствия № СФ/121-1859 от 17.06.2012 Средство УЦ: "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 Заключение на средство УЦ: Сертификат соответствия № СФ/128-1822 от 01.06.2012
9. Расширение 2.5.29.32
Название: Политики сертификата
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1 [2]Политика сертификата: Идентификатор политики=Класс средства ЭП КС2
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: 0D47 F9D8 F0EE B4FE F915 5356 DECF F1CE 1275 A4E9 5973 1D99 F177 2453 DE0E 8DA5 1F86 B62C 024D 21F0 738F 604E 1774 DB30 91C5 B52B D14B 1727 8979 C98D 94B3 C9B9

Подпись владельца сертификата/полномочного представителя: _____/_____

"___" _____ 20__ г.

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

К настоящему заявлению прилагаются в электронной форме:

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

_____ _____ /_____/

«____» _____ 20____ г.

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

«___»_____20__ г.

М.П.

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

К настоящему заявлению прилагаются в электронной форме:

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

_____ _____ /_____/

«____» _____ 20____ г.

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

«___»_____20__ г.

М.П.

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

Реализуемые функции Сервиса электронной подписи ООО «КРИПТО-ПРО»

1. Назначение сервиса

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

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

2. Поддерживаемые форматы и стандарты

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

Поддерживаемые форматы криптографических сообщений:

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

3. Используемые средства электронной подписи

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

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

4. Предоставление доступа к сервису

Доступ к Сервису электронной подписи осуществляется круглосуточно в режиме 24x7 по каналам связи посредством Веб-интерфейса, предоставляемого Удостоверяющим центром, или Прикладного интерфейса, используемого для подключения Информационных систем Уполномоченной организации в соответствии с документом «ЖТЯИ.00082-01 90 02. ПАК «КриптоПро DSS». Версия 1.0. Руководство разработчика».

Аутентификация пользователей осуществляется с использованием штатного Центра идентификации в составе ПАК «КриптоПро DSS» или по протоколу SAML 2.0 (WS Security) с использованием Стороннего центра идентификации Уполномоченной организации, подключаемого к Сервису электронной подписи в соответствии с документом «ЖТЯИ.00082-01 90 01. ПАК «КриптоПро DSS». Версия 1.0. Руководство администратора».

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

Вторичная аутентификация пользователей осуществляется посредством одноразового кода, высылаемого Пользователям Удостоверяющего центра в информационном сообщении или формируемого с помощью OTP-токена.

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

5. Информирование Пользователей Удостоверяющего центра

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

6. Защита информации

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

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

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

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

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

7. Правила пользования Сервисом электронной подписи

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

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

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

Использование ключа электронной подписи в СЭП должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем УЦ) с помощью одноразового пароля, формируемого персональным OTP-токеном владельца

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

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

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

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

8. Аудит Сервиса электронной подписи

Регистрация всех операций, выполняемых Операторами и Пользователями Удостоверяющего центра, осуществляется средствами СЭП. Журналы аудита выгружаются средствами СЭП и используются для контроля и анализа выполненных операций при разборе спорных вопросов и разрешении конфликтных ситуаций.

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

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

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Подтверждает подключение к Сервису электронной подписи ООО «КРИПТО-ПРО» в соответствии с указанными значениями параметров функционирования:

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

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

28.	Сложность одноразовых паролей	1 – только цифры 2 – цифры и буквы, 3 – цифры и буквы в разном регистре, 4 – цифры, буквы в разном регистре и спец символы (по умолчанию – 1)
29.	Максимальное количество попыток ввода одноразового пароля	От 0 до 2147483647, 0 – блокирование отключено (по умолчанию – 3)
30.	Время действия одноразового пароля (в секундах)	От 1 до 2147483647 (по умолчанию 300)
31.	Минимальное время жизни одноразового пароля (в секундах) – до возможности запроса нового пароля, пока не введен старый.	От 1 до 2147483647 (по умолчанию 300)
32.	Максимальный размер поля с информацией о документе, попадающей в SMS (в символах)	От 0 до 256 (по умолчанию 256)
33.	Использование ПИН-кода для ключевого контейнера	Требовать/ Не требовать/Позволять задавать (по умолчанию - Позволять задавать)
34.	Перечень событий для рассылки уведомлений Пользователям и Операторам СЭП	Опционально. Перечислить требуемые в соответствии с Руководством Администратора ПАК «КриптоПро DSS» п. 9.1 Таблица 87, 88.
35.	Перечень адресов электронной почты и номеров мобильных телефонов для рассылки уведомлений Операторам о событиях СЭП	С условием получения разрешения от владельцев адресов и мобильных телефонов
36.	Дополнительные условия (кастомизация Web-интерфейса пользователя/оператора, иконка стороннего ЦИ, набор компонент имени отображаемых пользователю/оператору в Web - интерфейсе ЦИ, регистрация специальных OID и шаблонов сертификатов и т.п.)	Указывает УО

_____ _____ /_____/

«____» _____ 20____ г.

_____ _____ /_____/

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

«___»_____20__ г.

М.П.

Приложение №9
к Регламенту Удостоверяющего центра ООО «КРИПТО-ПРО»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи
(Схема обслуживания: распределенная с оператором СЭП)
(Форма заявления на регистрацию Оператора Стороннего центра идентификации)

Заявление на регистрацию Оператора Стороннего центра идентификации Уполномоченной организации

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

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

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

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

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

Просит использовать адрес электронной почты _____ и (или) номер мобильного телефона для отправки почтовых сообщений и SMS-сообщений через оператора сотовой связи с уведомлением о событиях Сервиса электронной подписи
_____
Код страны, код региона, номер телефона в формате +X-XXX-XXX-XX-XX

(указывается при необходимости такой рассылки)

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

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

М.П.