



**Акционерное общество
«Специализированный регистратор –
Держатель реестров акционеров газовой промышленности»**

АО «ДРАГА»

УТВЕРЖДАЮ

Генеральный директор АО «ДРАГА»

М.В.Мурашов



Приказ №137 от 27.09.2021

**Регламент Уполномоченной организации
по выпуску и управлению квалифицированными сертификатами
ключей проверки электронной подписи Пользователей
Удостоверяющего центра**

Редакция №4

г. Москва
2021



1. Сведения об Уполномоченной Организации.

Акционерное общество «Специализированный регистратор - Держатель реестров акционеров газовой промышленности», именуемое в дальнейшем «Уполномоченная организация», зарегистрировано на территории Российской Федерации. Свидетельство о регистрации № 756.621, выдано Московской регистрационной Палатой 30 августа 1994 г., Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037739162240, присвоен Инспекцией Министерства Российской Федерации по налогам и сборам № 27 по Юго-Западному административному округу г. Москвы 21 января 2003 г.

Реквизиты:

Полное наименование: Акционерное общество «Специализированный регистратор – Держатель реестров акционеров газовой промышленности»

Юридический адрес: Российская Федерация, г. Москва.

Фактический адрес: Российская Федерация, 117420, г. Москва, ул. Новочеремушкинская, д. 71/32.

Адрес для корреспонденции: Российская Федерация, 117420, г. Москва, ул. Новочеремушкинская, д. 71/32.

ИНН/КПП: 7704011964 / 772701001

ОГРН: 1037739162240 **ОКПО:** 40094956

Контактные телефоны, факс, адрес электронной почты:

тел. +7 (495) 719-40-44; e-mail: info@draga.ru

2. Сведения об Удостоверяющем центре.

Общество с ограниченной ответственностью «Такском», зарегистрировано на территории Российской Федерации в городе Москве. Свидетельство о регистрации № 095.830 выдано 22.02.2000 Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1027700071530 от 29.07.2002 г.

Удостоверяющий центр ООО «Такском» аккредитован в Министерстве связи и массовых коммуникаций Российской Федерации на соответствие требованиям Федерального закона от 06.04.2011 года №63-ФЗ "Об электронной подписи".

Реквизиты:

Полное наименование: Общество с ограниченной ответственностью «Такском»

Юридический адрес: 119034, г. Москва, Барыковский пер., д. 4, стр. 2

Адрес для корреспонденции: 127051, г. Москва, а/я 40

ИНН/КПП: 7704211201/ 770401001

ОГРН: 1027700071530

3. Сведения об Исполнителе

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дальнейшем «Исполнитель», зарегистрировано на территории Российской Федерации в городе Москва (Свидетельство о внесении записи в единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 01 июля 2002 года серия 77 №007360250 от 29.01.2003 г.).



Исполнитель осуществляет свою деятельность на территории Российской Федерации на основании следующей лицензии: Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 12936 Н от 11 июня 2013 г. 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).

Реквизиты:

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

Юридический адрес: 105037, г. Москва, Измайловский проезд, д. 10, корп. 2, эт. 1, пом. IV

Адрес нахождения и для корреспонденции: 127018, г. Москва, ул. Сущевский Вал, д. 18

ИНН/КПП: 7717107991/771901001

ОГРН: 1037700085444

Контактные телефоны, факс, адрес электронной почты:

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



4. Термины и определения.

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

Исполнитель - Общество с ограниченной ответственностью «КРИПТО-ПРО», заключившее с Удостоверяющим центром договор оказания услуг аккредитованного удостоверяющего центра и предоставляющее услуги, связанные с выпуском и управлением квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, а также услуги, связанные с подключением Операторов СЭП и сторонних центров идентификации в целях предоставления доступа к СЭП.

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

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

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Уполномоченной организации и заверенный печатью Уполномоченной Организации, либо документ, в электронной форме предоставляемый Пользователю УЦ посредством подключенной к СЭП Информационной системы УО и подписанный электронной подписью. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи.

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

Мобильное приложение DSS Client/MyDSS – приложение для смартфона, являющееся компонентом ПО «Модуль аутентификации DSS Client для ПАК «КриптоПро DSS» версии 2.0», устанавливаемый на мобильном устройстве Пользователей УЦ.

Оператор Сервиса электронной подписи (Оператор СЭП) — физическое лицо, действующее от имени Уполномоченной Организации, совершающее действия по регистрации пользователей в Сервисе электронной подписи и управлению параметрами



доступа пользователей к Сервису электронной подписи, а также принятию решений по выпуску и управлению квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра для использования в информационной системе Уполномоченной организации.

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем сертификата ключа проверки электронной подписи, и указанное в сертификате ключа проверки электронной подписи, присоединившееся к Регламенту Уполномоченной организации.

Регламент Уполномоченной организации по выпуску и управлению квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра (Регламент) – настоящий документ Уполномоченной организации, определяющий условия предоставления и правила пользования услугами по выпуску и управлению сертификатов ключей проверки электронной подписи, получения доступа и правила пользования Сервисом электронной подписи для Пользователей УЦ.

Сервис электронной подписи (СЭП, Сервис) – комплекс организационных, технических и программных средств Исполнителя, обеспечивающих для Пользователей УЦ удаленную реализацию функций централизованного создания и хранения ключей электронной подписи, формирования и проверки усиленной квалифицированной электронной подписи электронных документов, аутентификации владельцев сертификатов ключей проверки электронной подписи при осуществлении доступа к СЭП и выполнении операций с использованием принадлежащих им ключей электронной подписи.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Средства криптографической защиты информации (СКЗИ) – средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

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.

Сторона, присоединившаяся к Регламенту (Клиент) – физическое лицо, в том числе индивидуальный предприниматель или лицо, занимающееся частной практикой, присоединившееся к настоящему Регламенту в порядке, предусмотренном настоящим Регламентом.



Удостоверяющий центр – аккредитованный в соответствии с Федеральным законом от 06.04.2011 г. №63-ФЗ «Об электронной подписи» удостоверяющий центр, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей.

Уполномоченная организация (Уполномоченная Организация) – Акционерное общество «Специализированный регистратор — Держатель реестров акционеров газовой промышленности», наделенное на основании заключенных договоров полномочиями по принятию решений о выпуске и управлении квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, а также управлению доступом к Сервису электронной подписи.

Электронная подпись (ЭП) – информация 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 (ЭД) – 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.

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



5. Общие положения.

5.1. Статус Регламента.

5.1.1. Настоящий Регламент Уполномоченной организации по выпуску и управлению квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

5.1.2. Сторонами Регламента (далее Стороны) являются Акционерное общество «Специализированный регистратор – Держатель реестров акционеров газовой промышленности», представляющее Уполномоченную организацию и Сторона, присоединившаяся к Регламенту.

5.1.3. Любое заинтересованное лицо может ознакомиться с Регламентом в офисе Уполномоченной организации по адресу: г. Москва, ул. Новочеремушкинская, д. 71/32, а также на сайте Уполномоченной организации: <https://draga.ru/>.

5.2. Присоединение к Регламенту.

5.2.1. Присоединение к Регламенту осуществляется путем подписания и предоставления Уполномоченной организации Заявления по форме Приложения № 1 к настоящему Регламенту.

5.2.2. Факт присоединения Стороны к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Заявления о присоединении к Регламенту.

5.2.3. После присоединения к Регламенту в установленном порядке Стороны вступают в соответствующие договорные отношения без ограничения срока действия.

5.2.4. Каждая из Сторон вправе без обращения в суд расторгнуть договор, письменно уведомив другую сторону за 30 календарных дней до дня расторжения. При этом Стороны в течение срока предупреждения до дня прекращения договора обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с настоящим Регламентом.

5.2.5. Прекращение действия договора не освобождает стороны от исполнения обязательств, возникших до указанного дня прекращения действия договора, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

5.3. Применение Регламента.

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

5.3.2. 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.

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

5.4. Изменение (дополнение) Регламента.

5.4.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Уполномоченной организацией в одностороннем порядке.

5.4.2. Уведомление присоединившейся Стороны о внесении изменений (дополнений) в Регламент осуществляется путем размещения указанных изменений на сайте Уполномоченной организации по адресу: <https://draga.ru/>



5.4.3. Все изменения (дополнения), вносимые Уполномоченной организацией в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу с даты размещения указанных изменений на сайте Уполномоченной организации.

5.4.4. Все изменения (дополнения), вносимые Уполномоченной организацией в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

5.4.5. Любые изменения и дополнения 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 (дополнений) в силу. В случае несогласия с изменениями (дополнениями) пользователь Удостоверяющего центра имеет право на расторжение своего присоединения к Регламенту в порядке, предусмотренном настоящим Регламентом.

5.4.6. Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

5.5. Пользователи УЦ и владельцы сертификатов.

5.5.1. Уполномоченная организация осуществляет выпуск сертификатов ключей проверки электронной подписи и предоставляет доступ к СЭП:

- работникам Уполномоченной организации;
- физическим лицам, в том числе индивидуальным предпринимателям (ИП) и уполномоченным представителям юридических лиц, являющимся клиентами Уполномоченной организации, присоединившимся к настоящему Регламенту.

5.5.2. В случае использования квалифицированной электронной подписи юридическим лицом, применяется подпись с указанием в качестве владельца квалифицированного сертификата ключа проверки электронной подписи физического лица, действующего от имени юридического лица без доверенности.

В случае, если от имени юридического лица действует лицо, не являющееся уполномоченным на действия от имени данного юридического лица без доверенности, электронный документ подписывается квалифицированной электронной подписью физического лица, являющегося таким представителем юридического лица, на основании доверенности выданной в соответствии с законодательством Российской Федерации.



6. Предоставление документов и информации.

6.1. Присоединяющаяся к Регламенту Сторона обязана предоставить Оператору СЭП документы, подтверждающие сведения, необходимые для идентификации Пользователя УЦ, в том числе признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность:

6.1.1. Если Сторона (заявитель), намеревающаяся стать владельцем сертификата ключа проверки электронной подписи, является физическим лицом:

- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность;
- страховой номер индивидуального лицевого счета заявителя - физического лица или его нотариальная копия;
- идентификационный номер налогоплательщика заявителя - физического лица или его нотариальная копия.

6.1.2. Если Сторона (заявитель), намеревающаяся стать владельцем сертификата ключа проверки электронной подписи, является индивидуальным предпринимателем:

- основной документ, удостоверяющий личность заявителя;
- страховой номер индивидуального лицевого счета заявителя - физического лица или его нотариальная копия;
- идентификационный номер налогоплательщика заявителя - физического лица или его нотариальная копия;
- свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя или его нотариальная копия;
- выписки из Единого государственного реестра индивидуальных предпринимателей, полученная не ранее чем за тридцать дней до ее представления.

6.2. Присоединяясь к настоящему Регламенту, Сторона в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» поручает Уполномоченной организации и Удостоверяющему центру в лице их уполномоченных работников и иных лиц, привлекаемых Уполномоченной организацией и Удостоверяющим центром, совершать с персональными данными, содержащимися в документах, представленных Стороной Уполномоченной организации для присоединения к настоящему Регламенту, а также в документах, которые будут представлены Уполномоченной организацией и 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 Уполномоченной организации и Удостоверяющего центра, обезличивание, блокирование, удаление, уничтожение персональных данных (далее – «обработка») в целях принятия Уполномоченной организацией и Удостоверяющим центром решения о возможности присоединения Клиентом к Регламенту, доступа к СЭП, в целях исполнения Регламента, реализации вытекающих из Регламента прав и обязанностей, а также в целях осуществления Уполномоченной организацией и Удостоверяющим центром функций, возложенных законодательством Российской Федерации.

6.3. Присоединяясь к настоящему Регламенту, Сторона подтверждает, что персональные данные, содержащиеся в представляемых Клиентом Уполномоченной организации документах, не являются тайной частной жизни, личной и/или семейной тайной субъектов персональных данных.



6.4. Сторона поручает Уполномоченной организации и 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 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», с соблюдением конфиденциальности персональных данных и обеспечением безопасности персональных данных при их обработке, на безвозмездной основе.

6.5. Сторона выражает в письменном виде свое согласие с тем, что персональные данные содержащиеся в представленных Уполномоченной организации документах, обрабатываются Уполномоченной организацией и Удостоверяющим центром с согласия Стороны в указанных выше целях, а также гарантирует, что документы, содержащие персональные данные Стороны, будут представляться Уполномоченной организации и Удостоверяющему центру в соответствии с настоящим Регламентом. Стороне разъяснены юридические последствия в случае отказа Стороной от предоставления письменного согласия на обработку персональных данных, заключающиеся в том, что Уполномоченная организация и Удостоверяющий центр вынуждены будут отказать Стороне в регистрации пользователя УЦ и выпуске сертификата ключа проверки электронной подписи.

6.6. Сторона выражает в письменном виде свое согласие с тем, что персональные данные, заносямые в сертификаты ключей проверки электронной подписи, владельцами которых они являются, относятся к общедоступным персональным данным, разрешенным для распространения с соблюдением запретов и условий, указанных в письменном согласии Стороны.

6.7. 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 Уполномоченной организацией и Удостоверяющим центром самостоятельно с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».



7. Права и обязанности сторон.

7.1. Уполномоченная организация обязана:

7.1.1. Обеспечить предоставление доступа Пользователям УЦ к Сервису электронной подписи с применением многофакторной аутентификации.

7.1.2. Обеспечить посредством отправки SMS-сообщений уведомление Пользователей УЦ о выполняемых от их имени операциях с использованием Сервиса электронной подписи.

7.1.3. Обеспечить конфиденциальность аутентификационных данных Пользователей УЦ и информации, передаваемой в составе SMS-сообщений посредством SMS-шлюза Уполномоченной организации.

7.2. Оператор СЭП обязан:

7.2.1. Обеспечить регистрацию Пользователей в Сервисе электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

7.2.2. Обеспечить посредством Сервиса электронной подписи создание и хранение ключа электронной подписи и соответствующего сертификата ключа проверки электронной подписи зарегистрированного в Удостоверяющем центре лица по Заявлению на выдачу квалифицированного сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

7.2.3. Предоставить Пользователю УЦ сертификат ключа проверки электронной подписи.

7.2.4. Прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по Заявлению на прекращение действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

7.3. Сторона, присоединившаяся к Регламенту, обязана:

7.3.1. Известить Уполномоченную организацию об изменениях идентификационных данных Пользователя и предоставить документы, предусмотренные настоящим Регламентом, в течение 5-ти рабочих дней с момента регистрации изменений.

7.3.2. С целью обеспечения гарантированного ознакомления Пользователей УЦ, с полным текстом Регламента не реже одного раза в тридцать календарных дней обращаться на сайт Уполномоченной организации по адресу: <https://draga.ru> - за сведениями об изменениях в Регламенте.

7.3.3. Пользователь Удостоверяющего центра, являющийся полномочным представителем присоединившейся Стороны обязан:

7.3.3.1. Создавать и хранить сформированный ключ электронной подписи исключительно с использованием Сервиса электронной подписи в неэкспортируемом формате, т.е. недоступном для сохранения и использования на съемных ключевых носителях и рабочем месте пользователя.

7.3.3.2. Устанавливать и хранить в тайне персональный код для защиты доступа к ключу электронной подписи.

7.3.3.3. Устанавливать и хранить в тайне персональный пароль для защиты доступа к СЭП.

7.3.3.4. Хранить в тайне аутентификационную информацию и обеспечить сохранность специальных средств, используемых для подтверждения доступа и выполнения операций в СЭП (мобильный телефон и SIM-карту для получения SMS-



уведомлений), принимать все возможные меры для предотвращения их раскрытия, искажения, потери и несанкционированного использования.

7.3.3.5. Применять для формирования электронной подписи только действующий персональный ключ электронной подписи.

7.3.3.6. Не применять персональный ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

7.3.3.7. Применять персональный ключ электронной подписи только в соответствии с областями использования, указанными в соответствующем данному ключу сертификате ключа проверки электронной подписи.

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

7.3.3.9. Не использовать персональный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, Заявление на прекращение действия которого подано Оператору СЭП, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия сертификата.

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

7.3.3.11. Не использовать персональный ключ электронной подписи до предоставления Оператору СЭП подписанной копии соответствующего сертификата ключа проверки электронной подписи.

7.4. Уполномоченная организация имеет право:

7.4.1. Заверять печатью и подписью сотрудника Уполномоченной организации копии сертификатов ключей проверки электронной подписи, созданных Оператором СЭП и выдаваемых сотрудником Уполномоченной организации Пользователю УЦ.

7.5. Оператор сервиса электронной подписи имеет право:

7.5.1. Отказать в регистрации в Сервисе электронной подписи уполномоченному представителю Стороны, присоединившейся к Регламенту, в случае ненадлежащего оформления необходимых регистрационных документов.

7.5.2. Отказать в создании сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления заявления на создание и выдачу сертификата ключа проверки электронной подписи.

7.5.3. Отказать в прекращении действия сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления заявления на прекращение действия сертификата ключа проверки электронной подписи.



7.5.4. Отказать в прекращении действия сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

7.5.5. Отказать в создании и выдаче сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если для формирования запроса на создание сертификата ключа проверки электронной подписи Пользователем УЦ не использовался Сервис электронной подписи.

7.6. Сторона, присоединившаяся к Регламенту, имеет право:

7.6.1. Получить сертификат ключа проверки электронной подписи Удостоверяющего центра.

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

7.6.3. Применять список отозванных сертификатов, созданный Удостоверяющим центром, для проверки статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

7.6.4. Воспользоваться подключенной к СЭП Информационной системой Уполномоченной организации для передачи по линиям связи Уполномоченной организации заявления на прекращение/ действия сертификата ключа проверки электронной подписи в электронном виде.

7.6.5. Использовать СЭП для создания электронной подписи с применением действующего сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром по решению Уполномоченной организации, посредством подключенной к СЭП Информационной системы Уполномоченной организации.

7.6.6. Получать уведомления о выполняемых операциях с персональным ключом электронной подписи, хранение которого осуществляется с использованием СЭП.

7.6.7. Применять одноразовый пароль, получаемый в SMS-сообщении на зарегистрированный Оператором СЭП номер мобильного телефона, для аутентификации при осуществлении доступа к СЭП и подтверждения применения персонального ключа электронной подписи, хранение которого осуществляется с использованием СЭП.

7.6.8. Обратиться к Оператору СЭП для прекращения действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи.



8. Ответственность сторон и Разрешение споров.

8.1. 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.

8.2. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

8.3. Сторонами в споре, в случае его возникновения, считаются Уполномоченная организация и Сторона, присоединившаяся к Регламенту.

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

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

8.6. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в Арбитражном суде.



9. Порядок предоставления и правила пользования Сервисом электронной подписи.

9.1. Регистрация Пользователей УЦ в Сервисе электронной подписи и выпуск Сертификата КЭП

Оператор СЭП осуществляет регистрацию Пользователя в Сервисе электронной подписи, создание и выпуск Сертификата ключа электронной подписи, только в том случае, если Сторона, полномочным представителем которой является регистрирующееся лицо, присоединилась к настоящему Регламенту путем предоставления документов, подтверждающих сведения, необходимые для идентификации Пользователя УЦ предусмотренных разделом 6 настоящего Регламента.

Регистрация Пользователя в Сервисе электронной подписи осуществляется на основании Заявления о присоединении к Регламенту Уполномоченной организации и регистрацию в Сервисе электронной подписи, (Приложение №1 к настоящему Регламенту), при личном обращении регистрирующегося физического лица в офис Уполномоченной организации.

В целях получения сертификата ключа проверки КЭП в соответствии с требованиями Регламента лицу, который будет являться Пользователем УЦ и владельцем сертификата ключа проверки электронной подписи, необходимо предоставить в адрес Регистратора:

- Заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи (Приложение №2 к настоящему Регламенту);
- документы, предусмотренные разделом 6 настоящего Регламента;
- подтверждение оплаты услуг выдачи сертификата ключа проверки электронной подписи.

После осуществления процедуры идентификации обратившегося лица, на основании документа, признаваемого в соответствии с законодательством Российской Федерации документом, удостоверяющим личность, либо путем установления личности и полномочий представителя юридического лица, а также проверки и анализа предоставленных документов, осуществляется их дальнейшее рассмотрение.

Обработка предоставленных Заявлений и документов осуществляется в течение 1 (одного) часа с момента их приема и регистрации.

По итогам проведенной экспертизы предоставленных в соответствии с Регламентом документов и принятии положительного решения о регистрации обратившегося лица в сервисе, Оператор СЭП выполняет действия по занесению информации в Сервис электронной подписи и созданию Сертификата КЭП:

- регистрирует Пользователя УЦ в Сервисе электронной подписи;
- на основании указанной в Заявлении информации устанавливает *Кодовое слово* – любое секретное слово, число или их комбинация, указанное в Заявлении и используемое для дополнительной идентификации Пользователя УЦ в СЭП
- с использованием СЭП формирует запрос и подтверждает создание ключа КЭП и Сертификата ключа проверки ЭП.



По окончании процедуры регистрации Пользователя УЦ в СЭП и создания Сертификата ключа проверки КЭП, уполномоченный сотрудник Регистратора, предоставляет Пользователю УЦ:

- Информацию о регистрации Пользователя в СЭП, содержащую логин и временный пароль для доступа к сервису посредством подключенной Информационной системы Уполномоченной организации, и QR-код для активации ключа электронной подписи в мобильном приложении DSS Client/MyDSS. Форма приведена в Приложении №5 к настоящему Регламенту;
- копию сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе. Копии сертификата ключа проверки электронной подписи на бумажном носителе формируются в двух экземплярах, заверяются собственноручной подписью лица, проходящего процедуру регистрации, а также печатью и подписью сотрудника Уполномоченной организации;
- Руководство по обеспечению безопасности использования КЭП.

В случае отказа в регистрации, заявителю предоставляется письменный документ с указанием причин отказа и рекомендаций по их устранению.

9.2. Изменение регистрационных данных Пользователя УЦ.

В случае изменения регистрационных данных, указанных в Заявлении при регистрации Пользователя в СЭП, в т.ч. номера мобильного телефона для отправки SMS-сообщений с уведомлением о выполняемых операциях с использованием электронной подписи или изменения способа подтверждения использования ключа электронной подписи Пользователя УЦ (отправка кода подтверждения в SMS-сообщении на номер мобильного телефона), необходимо внести соответствующие изменения в информацию, содержащуюся в Сервисе электронной подписи, путем подачи заявления по форме, предусмотренной Приложением № 3 к настоящему Регламенту.

Внесение изменений в регистрационные данные Пользователя УЦ осуществляется Оператором СЭП на основании *Заявления на изменение регистрационных данных Пользователя Удостоверяющего центра (Приложение №3)*.

Заявление может подаваться в бумажной форме при личном прибытии Пользователя УЦ в офис Уполномоченной организации и в электронной форме, посредством подключенной к СЭП Информационной системы Уполномоченной Организации.

9.2.1. Внесение изменений в регистрационные данные Пользователя по заявлению, поданному в бумажной форме.

Форма заявления на изменение регистрационных данных Пользователя УЦ в сервисе электронной подписи приведена в Приложении № 3 к настоящему Регламенту.

По итогам осуществления процедуры идентификации обратившегося лица, на основании документа, признаваемого в соответствии с законодательством Российской Федерации документом, удостоверяющим личность, либо путем установления полномочий представителя юридического лица, документы подлежат дальнейшему рассмотрению и обработке Оператором СЭП.

Заявление на изменение регистрационных данных Пользователя УЦ рассматривается Оператором СЭП в течение 1 (одного) часа с момента его поступления.



В случае отказа во внесении изменений в регистрационные данные Пользователя, заявителю предоставляется письменный документ, с указанием причин отказа и рекомендаций по их устранению.

При принятии положительного решения, Оператор СЭП подтверждает внесение изменений и актуализацию регистрационных данных Пользователя в соответствии с предоставленными документами путем направления информационного сообщения посредством подключенной к СЭП Информационной системы Уполномоченной Организации в срок, установленный для рассмотрения заявления.

9.2.2. Внесение изменений в регистрационные данные Пользователя по заявлению, поданному в электронной форме.

Подача Пользователем УЦ заявления на изменение регистрационных данных Пользователя в Сервисе электронной подписи осуществляется посредством подключенной к СЭП Информационной системы Уполномоченной Организации.

Заявление на изменение регистрационных данных Пользователя Удостоверяющего центра в электронной форме представляет собой электронный документ, с подписью на действующем ключе электронной подписи Пользователя УЦ.

Значения полей, содержащиеся в запросе должны быть идентичны значениям этих полей в сертификате ключа проверки электронной подписи, соответствующего ключу электронной подписи Пользователя УЦ, которым сформирована электронная подпись в заявлении.

После получения заявления Оператор СЭП проверяет корректность электронной подписи, которой подписано заявление, устанавливает его автора, сравнивает значения полей, содержащихся в предоставленном Заявлении, со значениями, указанными в сертификате ключа проверки электронной подписи автора настоящего заявления.

Срок рассмотрения заявления составляет 1 (один) рабочий день с момента получения заявления.

В случае отрицательного результата проведенных проверок, Оператор СЭП отклоняет заявление на изменение регистрационных данных Пользователя и уведомляет об этом Пользователя УЦ, посредством подключенной к СЭП Информационной системы Уполномоченной Организации в срок, установленный для рассмотрения заявления.

При принятии положительного решения, Оператор СЭП принимает заявление и осуществляет внесение изменений и актуализацию регистрационных данных Пользователя в соответствии с предоставленными документами.

По итогам внесения изменений и актуализации регистрационных данных в соответствии с предоставленными документами, Пользователь УЦ, посредством подключенной к СЭП Информационной системы Уполномоченной Организации, получает электронный документ, подписанный Оператором СЭП.

Информация, подтверждающая ознакомление Пользователя с информацией, содержащейся в сертификате ключа проверки электронной подписи, хранится у Оператора УЦ.

9.3. Создание (смена) ключа электронной подписи и сертификата ключа проверки электронной подписи.

Создание ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется при его плановой либо внеплановой замене в соответствии с положениями и формами документов, утвержденными настоящим Регламентом.



Формирование ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется Оператором СЭП на основании Заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи (Приложение №2 к настоящему Регламенту).

Заявление на выдачу сертификата ключа проверки электронной подписи подаётся в бумажной форме при личном прибытии Пользователя УЦ в офис Уполномоченной организации.

Форма *Заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи* приведена в Приложении № 2 к настоящему Регламенту.

По итогам осуществления процедуры идентификации обратившегося лица, по документу, признаваемому в соответствии с законодательством Российской Федерации документом, удостоверяющим личность, либо путем установления личности и полномочий представителя юридического лица, документы подлежат дальнейшему рассмотрению и обработке Оператором СЭП.

Заявление на выдачу квалифицированного сертификата ключа электронной подписи рассматривается Оператором СЭП в течение 1 (одного) часа с момента его поступления.

В случае отказа в выдаче ключа электронной подписи и сертификата ключа проверки электронной подписи, заявителю предоставляется письменный документ, с указанием причин отказа и рекомендаций по их устранению.

При принятии положительного решения, Оператор СЭП подтверждает создание ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ посредством Сервиса электронной подписи.

Копии сертификата ключа проверки электронной подписи на бумажном носителе формируются в двух экземплярах, заверяются собственноручной подписью лица, проходящего процедуру регистрации, а также печатью и подписью Оператора СЭП.

По окончании процедуры создания ключа и сертификата ключа проверки электронной подписи, один экземпляр копии сертификата ключа проверки электронной подписи на бумажном носителе выдается Пользователю УЦ.

9.4. Прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

9.4.1. Основания прекращения действия квалифицированного сертификата

Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.



Для прекращения действия сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на прекращение действия сертификата ключа проверки электронной подписи Оператору СЭП.

Заявление на прекращение действия сертификата ключа проверки электронной подписи может подаваться в бумажной форме при личном прибытии Пользователя УЦ к Оператору СЭП в офис Уполномоченной Организации, либо в электронной форме с использованием Сервиса электронной подписи (посредством подключенной к СЭП Информационной системы Уполномоченной Организации).

9.4.2. Прекращение действия сертификата ключа проверки электронной подписи по заявлению, поданному в бумажной форме.

Форма *Заявления на прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра* приведена в Приложении № 4 к настоящему Регламенту.

Заявление на прекращение действия сертификата ключа проверки электронной подписи заверяется собственноручной подписью владельца сертификата ключа проверки электронной подписи Пользователя УЦ и подается в офисе Уполномоченной Организации.

Обработка заявления на прекращение действия сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ о прекращении действия сертификата ключа проверки электронной подписи осуществляются в сроки, установленные Удостоверяющим центром.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено, указанное в поле `thisUpdate` изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в создаваемые Удостоверяющим центром сертификаты ключей проверки электронной подписи в поле `CRL Distribution Point`.

9.4.3. Прекращение действия сертификата ключа проверки электронной подписи по заявлению, поданному в электронной форме.

Подача Пользователем УЦ заявления на прекращение действия сертификата ключа проверки электронной подписи в электронной форме осуществляется с использованием Сервиса электронной подписи посредством подключенной к СЭП Информационной системы Уполномоченной Организации.

В качестве подписываемых данных используется запрос на прекращение действия сертификата ключа проверки электронной подписи, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя УЦ.

После получения заявления Оператор СЭП проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа проверки электронной подписи, серийный номер которого указан в запросе на прекращение действия сертификата ключа проверки электронной подписи.

В случае отрицательного результата проведенных проверок, Оператор СЭП отклоняет заявление на прекращение действия сертификата ключа проверки электронной подписи и уведомляет об этом Пользователя УЦ, посредством подключенной к СЭП Информационной системы Уполномоченной Организации.



При принятии положительного решения, Оператор СЭП направляет Заявление на дальнейшую обработку в УЦ.

Обработка заявления на прекращение действия сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ о прекращении действия сертификата ключа проверки электронной подписи осуществляются в сроки, установленные Удостоверяющим центром.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено, указанное в поле `thisUpdate` изданного списка отозванных сертификатов.

9.5. Управление доступом к СЭП.

Доступ Пользователей УЦ к Сервису электронной подписи осуществляется посредством Информационной системы Уполномоченной организации.

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

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

9.6. Прочие условия.

Период времени действия ключа электронной подписи, соответствующего выданному сертификату ключа проверки электронной подписи Пользователя УЦ, являющегося юридическим лицом, должен находиться в пределах периода времени, на который Стороной, присоединившейся к Регламенту, выдана соответствующая доверенность на совершение действий, определенных положениями настоящего Регламента.



10. Форма сертификатов ключей проверки электронной подписи и сроки действия ключевых документов.

Форма сертификата ключа проверки электронной подписи соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи», создается Удостоверяющим центром в соответствии с Порядком реализации функций Удостоверяющего центра.

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

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

10.1. Сроки действия ключевых документов.

Срок действия ключа электронной подписи Удостоверяющего центра составляет 1 (один) год и 3 месяца.

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

В соответствии с требованиями Приказа ФСБ России № 796 от 27 декабря 2011 года о том, что срок действия Ключа проверки электронной подписи не должен превышать срок действия соответствующего ключа электронной подписи более чем на 15 лет, максимально допустимый срок действия Сертификата Удостоверяющего центра составляет 16 лет.

Срок действия ключа электронной подписи составляет 1 (один) год и 3 месяца.

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

Срок действия сертификата устанавливается УЦ в момент его изготовления.



11. Дополнительные положения.

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

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра действие сертификата ключа проверки электронной подписи Удостоверяющего Центра прекращается, Пользователи УЦ 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.

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

11.2. Конфиденциальность информации.

11.2.1. Типы конфиденциальной информации.

Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр осуществляет хранение созданных с использованием СЭП ключей электронной подписи Пользователей Удостоверяющего центра.

Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, и содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке (распространению, публикации) в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

Информация, передаваемая в составе электронного документа или SMS-сообщения при взаимодействии с Сервисом электронной подписи, считается конфиденциальной.

11.2.2. Типы информации, не являющейся конфиденциальной.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

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

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

Персональные данные, включаемые в сертификаты ключей проверки электронной подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.



11.2.3. Исключительные полномочия Уполномоченной Организации и Удостоверяющего центра

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

11.3. Форс-мажор.

11.3.1. 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.

11.3.2. 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.

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

11.3.4. 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.

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

11.3.6. 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.



12. Список приложений.

Приложение №1. Форма Заявление о присоединении к Регламенту Уполномоченной организации и регистрацию в Сервисе электронной подписи.

Приложение №2. Форма Заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи.

Приложение №3. Форма заявления на изменение регистрационных данных Пользователя в Сервисе электронной подписи.

Приложение №4. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи

Приложение №5. Информация о регистрации Пользователя в Сервисе электронной подписи (Пример).

Приложение №6. Реализуемые функции Сервиса электронной подписи.



Приложение №1 к Регламенту
Форма Заявления о присоединении к Регламенту Уполномоченной организации и
регистрацию Пользователя в Сервисе электронной подписи

**Заявление о присоединении к Регламенту
Уполномоченной организации и
регистрацию Пользователя в Сервисе электронной подписи**

Я, _____
(фамилия, имя, отчество (если имеется))

(серия и номер паспорта, кем и когда выдан)

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к **Регламенту Уполномоченной организации по выпуску и управлению квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра** (далее Регламент). С настоящим Регламентом и приложениями к нему ознакомлен и являюсь Стороной Регламента с момента подписания настоящего Заявления.

Прошу зарегистрировать в Сервисе электронной подписи, в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	Фамилия Имя Отчество (если имеется) заявителя	
E-Mail (E)	Адрес электронной почты заявителя	
Surname	Фамилия заявителя	
GivenName	Имя и отчество (если имеется) заявителя	
INN	ИНН (индивидуальный номер налогоплательщика) заявителя	
SNILS	СНИЛС (страховой номер индивидуального лицевого счета) заявителя	
Locality (L)	Наименование населенного пункта по адресу регистрации	
State (S)	Субъект Российской Федерации по адресу регистрации	
OGRNIP ¹	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

и наделить полномочиями Пользователя УЦ, установленными Регламентом УО.

Настоящим выражаю согласие с обработкой Удостоверяющим центром, Исполнителем и Уполномоченной организацией своих персональных данных и признаю, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным.

Поручаю Исполнителю хранение ключей электронной подписи, выданных с использованием Сервиса электронной подписи, подписания с их помощью электронных документов и передачи подписанных электронных документов Уполномоченной организации по моим волеизъявлениям в установленном настоящим Регламентом порядке.

¹ Указывается только для индивидуальных предпринимателей



Регламент Уполномоченной организации по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
Пользователей Удостоверяющего центра

Подтверждаю, что с правилами работы Сервиса электронной подписи ознакомлен, возникающие при использовании СЭП требования и обязанности признаю, принимаю и обязуюсь исполнять надлежащим образом.

Прошу установить следующее Кодовое слово _____,
используемое для дополнительной идентификации Пользователя УЦ в СЭП.

Прошу использовать номер мобильного телефона для отправки через оператора сотовой связи SMS-сообщений с уведомлением о выполняемых от моего имени операциях с использованием Сервиса электронной подписи _____

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

Прошу использовать указанный выше телефонный номер для отправки одноразового кода подтверждения моего волеизъявления о подписании электронных документов с применением принадлежащего мне ключа электронной подписи посредством Сервиса электронной подписи

Обязуюсь обеспечить сохранность мобильного телефона и sim-карты с указанным номером от доступа третьих лиц.

(подпись)

(фамилия, инициалы)

« _____ » _____ 20__ года
дата



Приложение №2 к Регламенту

Форма Заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи

Заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи

Я, _____, заявляю об
акцепте действующего на дату регистрации Заявления «Порядка реализации функций
Аккредитованного Удостоверяющего ООО «Такском» и исполнения его обязанностей»
(размещенного на сайте Удостоверяющего центра по адресу <https://taxcom.ru>) в порядке,
предусмотренном ст. 428 Гражданского Кодекса Российской Федерации и прошу создать
квалифицированный сертификат ключа проверки электронной подписи (далее
квалифицированный сертификат) в соответствии со следующими данными:

Сведения о физическом лице – Пользователе Аккредитованного удостоверяющего центра	
Фамилия	
Имя	
Отчество	
Пол	
Дата рождения	
СНИЛС	
ИНН	
ОГРНИП (заполняется только ИП)	
Гражданство	Россия
Документ, удостоверяющий личность	Тип документа: _____ серия _____ номер _____ дата выдачи _____ выдан _____ код подразделения (при наличии) _____
Город	
Субъект РФ	
Страна	
Контактный телефон	
Адрес электронной почты	

Настоящим выражаю согласие с обработкой своих персональных данных ООО «Такском», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение). Персональные данные, на обработку которых дается согласие в целях исполнения договора, предусматривающего оказание услуг удостоверяющего центра в соответствии с федеральным законом от 06.04.2008 №63-ФЗ «Об электронной подписи» (далее ФЗ «Об электронной подписи») для изготовления квалифицированных сертификатов: фамилия, имя, отчество, ИНН, СНИЛС, место работы (организация), подразделение, должность, адрес места жительства, адрес электронной почты, пол, абонентский номер, паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации). Соглашаюсь с указанием своих персональных данных согласно приказу Минкомсвязи РФ от 05.10.2011 № 250 в реестре выданных ООО «Такском» квалифицированных сертификатов, при этом признаю, что в соответствии с п. 3 ст. 15 ФЗ «Об электронной подписи» ООО «Такском» обязан обеспечить любому лицу безвозмездный доступ к реестру квалифицированных сертификатов ООО «Такском». Соглашаюсь с передачей своих персональных данных в Единую систему идентификации и аутентификации в целях обеспечения требования ч. 5 ст. 18 ФЗ «Об электронной подписи».

« ____ » _____ 20__ г.

подпись



Приложение №3 к Регламенту
Форма Заявления на изменение регистрационных данных Пользователя УЦ
в Сервисе электронной подписи

Заявление на изменение регистрационных данных Пользователя УЦ в Сервисе электронной подписи

Я, _____
(фамилия, имя, отчество (если имеется))

(серия и номер паспорта, кем и когда выдан)

Прошу внести изменения в информацию, содержащуюся в Сервисе электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	Фамилия Имя Отчество (если имеется) заявителя	
E-Mail (E)	Адрес электронной почты заявителя	
Surname	Фамилия заявителя	
GivenName	Имя и отчество (если имеется) заявителя	
INN	ИНН (индивидуальный номер налогоплательщика) заявителя	
SNILS	СНИЛС (страховой номер индивидуального лицевого счета) заявителя	
Locality (L)	Наименование населенного пункта по адресу регистрации	
State (S)	Субъект Российской Федерации по адресу регистрации	
OGRNIP ²	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

Настоящим выражаю согласие с обработкой Уполномоченной организацией своих персональных данных и признаю, что персональные данные, владельцем которых я являюсь, относятся к общедоступным персональным данным.

С Регламентом Уполномоченной организации и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Подтверждаю, что с правилами работы Сервиса электронной подписи ознакомлен, возникающие при использовании СЭП требования и обязанности признаю, принимаю и обязуюсь исполнять надлежащим образом.

Прошу установить следующее Кодовое слово _____,
используемое для дополнительной идентификации Пользователя УЦ в СЭП.

Прошу использовать номер мобильного телефона для отправки через оператора сотовой связи SMS-сообщений с уведомлением о выполняемых от моего имени операциях с использованием Сервиса электронной подписи _____

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

² Указывается только для индивидуальных предпринимателей



Регламент Уполномоченной организации по выпуску и управлению
квалифицированными сертификатами ключей проверки электронной подписи
Пользователей Удостоверяющего центра

Прошу использовать указанный выше телефонный номер для отправки одноразового кода подтверждения моего волеизъявления о подписании электронных документов с применением принадлежащего мне ключа электронной подписи посредством Сервиса электронной подписи

Обязуюсь обеспечить сохранность мобильного телефона и sim-карты с указанным номером от доступа третьих лиц.

(подпись)

(фамилия, инициалы)

« _____ » _____ 20__ года
дата



Приложение №4 к Регламенту
Форма заявления на прекращение действия сертификата ключа проверки
электронной подписи

**Заявление на прекращение действия сертификата ключа проверки
электронной подписи**

Я, _____,
(фамилия, имя, отчество (если имеется))

Паспорт серии _____ № _____ Выдан « _____ » _____ года

(наименование органа, выдавшего документ)

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

Серийный номер сертификата	
Фамилия	
Имя	
Отчество	
СНИЛС	

(подпись) / _____
(Ф.И.О. заявителя)

« _____ » _____ 20__ года
(дата)



Информация о регистрации Пользователя в Сервисе электронной подписи

На основании предоставленного Заявления на регистрацию Пользователя в Сервисе электронной подписи и в соответствии с указанными в нем идентификационными данными:

(фамилия, имя, отчество)

Вам предоставлены:

Логин	ReG20160908
Пароль	ST08092016
QR - код для активации ключа электронной подписи в мобильном приложении <u>DSS Client/MyDSS</u>	

С порядком подключения Пользователем УЦ вторичной аутентификации с использованием мобильного приложения DSS Client/MyDSS можно ознакомиться на официальном сайте АО «ДРАГА» - <https://draga.ru>.

Предоставленный Оператором СЭП (временный) пароль подлежит замене на постоянный (собственный) при первичном использовании СЭП Пользователем УЦ.

Сохранность и неразглашение полученного логина/пароля обеспечивается Пользователем УЦ.

В случае утери логина/пароля или возникновения подозрения о том, что логином/паролем воспользовалось постороннее лицо, необходимо в течение одного рабочего дня уведомить Оператора СЭП о необходимости блокировки доступа к Сервису и аннулировании комбинации логин/пароль по телефону: 8(495)123-30-90.



Реализуемые функции Сервиса электронной подписи

1. Назначение сервиса

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

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

2. Поддерживаемые форматы и стандарты

Электронная подпись создается с использованием криптографических алгоритмов в соответствии с ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и 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. «Чистая» (необработанная) Электронная подпись ГОСТ 34.10 – 2001, ГОСТ 34.10 – 2012;
2. Усовершенствованная подпись в соответствии с ETSI TS 101 733 "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)", рекомендациями RFC 5652, "Cryptographic Message Syntax" (CAAdES-BES и CAAdES-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 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 Исполнителем, или Прикладного интерфейса, используемого для подключения Информационных систем



Уполномоченной организации в соответствии руководством разработчика программного обеспечения «КриптоПро DSS».

Аутентификация пользователей осуществляется с использованием штатного Центра идентификации в составе ПАК «КриптоПро DSS» или по протоколу SAML (WS Security) или OpenID с использованием Стороннего центра идентификации Уполномоченной организации, подключаемого к Сервису электронной подписи в соответствии с документацией на программное обеспечение «КриптоПро DSS».

Руководства доступны по адресу <https://www.cryptopro.ru>.

Вторичная аутентификация пользователей осуществляется посредством ключа аутентификации в мобильном приложении (программе для ЭВМ) «КриптоПро DSS Client» из состава ПО «Модуль аутентификации DSS Client для ПАК «КриптоПро DSS» версии 2.0» на устройствах Пользователей УЦ; одноразового кода, высылаемого Пользователям УЦ в информационном сообщении или формируемого с помощью OTP-токена.

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

5. Информирование Пользователей Удостоверяющего центра

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

6. Защита информации

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

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

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

Защита информации, передаваемой при подключении SMS-шлюза, осуществляется Уполномоченной организацией с использованием средств криптографической защиты, совместимых со средствами Удостоверяющего центра. Обеспечение информационной безопасности подтверждается аттестатом соответствия объекта информатизации автоматизированной системы Сервиса электронной подписи требованиям по защите информации от несанкционированного доступа.

7. Правила пользования Сервисом электронной подписи

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 может быть установлен индивидуальный PIN-код доступа к ключевому контейнеру, содержащему ключ электронной подписи.



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

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

Пользователь Удостоверяющего центра должен хранить в тайне индивидуальный PIN код доступа к ключевому контейнеру, аутентификационную информацию, обеспечить сохранность персональных средств аутентификации (ключ аутентификации для мобильного приложения (программы для ЭВМ) «КриптоПро DSS Client», 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 СЭП с заявлением на прекращение действия соответствующего сертификата ключа проверки электронной подписи в случае раскрытия, искажения персонального ключа электронной подписи, компрометации аутентификационной информации и утери специальных устройств, используемых для аутентификации (ключ аутентификации для мобильного приложения (программы для ЭВМ) «КриптоПро DSS Client», мобильного телефона, SIM-карты и (или) OTP-токена), а также в случае, если Пользователю Удостоверяющего центра стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе если Пользователь УЦ получил сообщение от СЭП о выполнении каких-либо операций от его имени в то время, когда он их не выполнял.

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

8. Аудит Сервиса электронной подписи

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