



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

АО «ДРАГА»

УТВЕРЖДАЮ

Генеральный директор АО «ДРАГА»



М.В.Мурашов

Приказ №55 от 21.04.2021

РЕГЛАМЕНТ

Уполномоченной организации Удостоверяющего центра ООО «КРИПТО-ПРО»

по выдаче и управлению квалифицированными сертификатами
ключей проверки электронной подписи, предоставлению доступа к Сервису
электронной подписи

Редакция №3

г. Москва
2021



1. Сведения об Уполномоченной Организации Удостоверяющего центра.

Акционерное общество «Специализированный регистратор - Держатель реестров акционеров газовой промышленности», именуемое в дальнейшем «Уполномоченная организация Удостоверяющего центра» («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. Новочеремушkinsкая, д. 71/32.

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

Банковские реквизиты:

- Банк ГПБ (АО) г. Москва
- БИК 044525823
- Р/с 40702810700000000026
- К/с 30101810200000000823

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 «КРИПТО-ПРО», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о регистрации № 001.602.749, выдано 16.11.1999г. Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003г., Свидетельство о внесении записи в ЕГРЮЛ в связи с государственной регистрацией изменений, вносимых в учредительные документы юридического лица за государственным регистрационным номером 2037719011031 от 12.03.2003г.

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>.



1. Сведения об Уполномоченной Организации Удостоверяющего центра.

Акционерное общество «Специализированный регистратор - Держатель реестров акционеров газовой промышленности», именуемое в дальнейшем «Уполномоченная организация Удостоверяющего центра» («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.

Банковские реквизиты:

- Банк ГПБ (АО) г. Москва
- БИК 044525823
- Р/с 40702810700000000026
- К/с 301018102000000000823

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 «КРИПТО-ПРО», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о регистрации № 001.602.749, выдано 16.11.1999г. Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003г., Свидетельство о внесении записи в ЕГРЮЛ в связи с государственной регистрацией изменений, вносимых в учредительные документы юридического лица за государственным регистрационным номером 2037719011031 от 12.03.2003г.

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>.



3. Термины и определения.

Удостоверяющий центр (УЦ) – 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 Удостоверяющего центра (Уполномоченная Организация) – Акционерное общество «Специализированный регистратор – Держатель реестров акционеров газовой промышленности», заключившее с Удостоверяющим центром договор, наделяющий данное юридическое лицо полномочиями по обеспечению создания, выдачи и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, управлению доступом к Сервису электронной подписи.

Сервис электронной подписи (СЭП) – комплекс организационных, технических и программных средств Удостоверяющего центра, обеспечивающих для Пользователей Удостоверяющего центра удаленную реализацию функций централизованного создания и 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.

Оператор Удостоверяющего центра (Оператор УЦ) – физическое лицо, являющееся работником Уполномоченной Организации, наделенное Удостоверяющим центром и Уполномоченной Организацией правами по осуществлению действий по регистрации и управлению сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра.

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем сертификата ключа проверки электронной подписи.

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

Информационная система – корпоративная информационная система, устройтелем которой является Уполномоченная Организация, в которой используются ключи электронной подписи и сертификаты ключей проверки электронной подписи посредством Сервиса электронной подписи, и предоставляющая определенные услуги участникам этой системы.

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 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. 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 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.

Регламент Уполномоченной организации по выдаче и управлению квалифицированными сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра "КРИПТО ПРО" (Регламент) – настоящий документ Уполномоченной организации, отражающий права и обязанности Пользователей УЦ и Операторов УЦ, протоколы работы, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования Удостоверяющего центра и Сервиса электронной подписи.

Реестр Удостоверяющего центра – реестр выданных Уполномоченной организацией Удостоверяющего центра квалифицированных сертификатов, также набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий:

- реестр выданных Уполномоченной организацией Удостоверяющего центра квалифицированных сертификатов;
- реестр заявлений на регистрацию пользователей в Удостоверяющем центре;

- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление 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.

Сертификат ключа проверки электронной подписи (Сертификат) - электронный документ, созданный Удостоверяющим центром, 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 Сервиса электронной подписи.

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, выданных 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 ответы, содержащие информацию о статусе сертификатов, выданных 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 (COC) – электронный документ с неквалифицированной 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.

Сторона, присоединившаяся к Регламенту (Клиент) – физическое лицо, в том числе индивидуальный предприниматель или лицо, занимающееся частной практикой, присоединившееся к настоящему Регламенту в порядке, предусмотренном разделом 4.2 Регламента.

КриптоПро myDSS – приложение для смартфона, позволяющее подписывать квалифицированной электронной подписью документы и контролировать действия Пользователя в СЭП. Обеспечивает строгую криптографическую аутентификацию пользователей, безопасное online-взаимодействие, отображение документа и подтверждение операций.

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

Электронная подпись (ЭП) – усиленная 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, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)» и RFC 7091 «GOST R 34.10-2012: Digital Signature Algorithm».

Online Certificate Status Protocol (OCSP) – протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».



Public Key Cryptography Standards (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 открытого ключа.

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) («служба коротких сообщений») — технология, позволяющая осуществлять приём и передачу коротких текстовых сообщений с помощью сотового (мобильного) телефона.

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



4. Общие положения.

4.1. Статус Регламента.

4.1.1. Настоящий Регламент Уполномоченной организации Удостоверяющего центра ООО «КРИПТО-ПРО» (далее – Регламент) является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

4.1.2. Сторонами Регламента (далее Стороны) являются Акционерное общество «Специализированный регистратор – Держатель реестров акционеров газовой промышленности», представляющее Уполномоченную организацию Удостоверяющего центра ООО «КРИПТО-ПРО», и Сторона, присоединившаяся к Регламенту.

4.1.3. 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/>.

4.2. Присоединение к Регламенту.

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

4.2.2. 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.

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

4.2.4. 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.

4.2.5. 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).

4.3. Применение Регламента.

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

4.3.2. 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.

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

4.4. Изменение (дополнение) Регламента.

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

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

4.4.3. 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.

4.4.4. 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.

4.4.5. 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 п.4.2.4. настоящего Регламента.

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

4.5. Пользователи УЦ и владельцы сертификатов.

4.5.1. Уполномоченная организация осуществляет выдачу 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.

4.5.2. 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.

4.5.3. Пользователем сертификата ключа проверки электронной подписи может быть любое физическое лицо или автоматизированная информационная система (устройство или программное приложение), в которой обрабатывается подписанная информация (электронный документ).

5. Предоставление документов и информации.

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

5.1.1. Если Сторона (заявитель), намеревающееся 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.

5.1.2. Если Сторона (заявитель), намеревающееся 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.

5.1. 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 организации 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.

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.

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.

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.

Сторона выражает в письменном виде свое согласие с тем, что персональные данные, заносимые 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.

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».



6. Права и обязанности сторон.

6.1. Уполномоченная организация обязана:

6.1.1. Обеспечить предоставление доступа Пользователей Удостоверяющего центра к Сервису электронной подписи с применением многофакторной аутентификации.

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

6.1.3. Обеспечить конфиденциальность аутентификационных данных Пользователей Удостоверяющего центра и информации, передаваемой в составе SMS-сообщений посредством SMS-шлюза Уполномоченной организации.

6.2. Оператор обязан:

6.2.1. Предоставить Пользователю Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра

6.2.2. Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

6.2.3. Обеспечить посредством Сервиса электронной подписи создание и хранение ключа электронной подписи и соответствующего сертификата ключа проверки электронной подписи зарегистрированного в Удостоверяющем центре лица по заявлениям на создание сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте и официально уведомить об этом владельца созданного сертификата ключа проверки электронной подписи.

6.2.4. 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.

6.2.5. Приостановить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на приостановление действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.2.6. Возобновить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на возобновление действия сертификата ключа проверки электронной подписи (исключительно в случае поступления заявления в период срока, на который действие сертификата было приостановлено), в соответствии с порядком, определенным в настоящем Регламенте.

6.3. Сторона, присоединившаяся к Регламенту, обязана:

6.3.1. Известить Уполномоченную организацию об изменениях данных Пользователя и предоставить документы, указанные в п. 5.1 настоящего Регламента, в течение 5-ти рабочих дней с момента регистрации изменений.

6.3.2. С целью обеспечения гарантированного ознакомления Пользователей Удостоверяющего центра, являющихся полномочным представителем присоединившейся Стороны, с полным текстом изменений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Уполномоченной организации по адресу: <https://draga.ru/akcioneram/dokumenty/reglament-upolnomochennoj-organizacii-udostoverjajushhego-centra-ooo-kripto-pro/> - за сведениями об изменениях в Регламенте.



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

6.3.3.1. 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.

6.3.3.2. Устанавливать и хранить в тайне персональный ПИН-код для защиты доступа к ключу электронной подписи.

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

6.3.3.4. 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.

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

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

6.3.3.7. Применять персональный ключ электронной подписи только в соответствии с областями использования, указанными в соответствующем данному ключу сертификате ключа проверки электронной подписи (поля Key Usage, Extended Key Usage сертификата ключа проверки электронной подписи).

6.3.3.8. Не применять персональный ключ электронной подписи и немедленно обратиться к Оператору УЦ с заявлением на приостановление/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.*

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

6.3.3.10. Не использовать персональный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, Заявление на приостановление действия которого подано Оператору УЦ, 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.

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



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

6.4. Уполномоченная организация имеет право:

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

6.5. Оператор Удостоверяющего центра имеет право:

6.5.1. Отказать в регистрации в Удостоверяющем центре уполномоченному представителю Стороны, присоединившейся к Регламенту, в случае ненадлежащего оформления необходимых регистрационных документов.

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

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

6.5.4. Отказать в приостановлении/возобновлении действия сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата ключа проверки электронной подписи.

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

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

6.5.7. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя УЦ с обязательным уведомлением владельца сертификата ключа проверки электронной подписи, действие которого приостановлено, и указанием обоснованных причин.

6.5.8. 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.

6.6. Сторона, присоединившаяся к Регламенту, имеет право:

6.6.1. Получить сертификат ключа проверки электронной подписи Удостоверяющего центра.

6.6.2. Получить список отозванных сертификатов, созданный Удостоверяющим центром.

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

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



- 6.6.5.** Применять сертификат ключа проверки электронной подписи Пользователя УЦ для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи.
- 6.6.6.** Воспользоваться подключенной к СЭП Информационной системой Уполномоченной организации для передачи по линиям связи Уполномоченной организации заявления на регистрацию в электронном виде.
- 6.6.7.** Воспользоваться подключенной к СЭП Информационной системой Уполномоченной организации для передачи по линиям связи Уполномоченной организации заявления на прекращение/приостановление/возобновление действия сертификата ключа проверки электронной подписи в электронном виде.
- 6.6.8.** Использовать СЭП для создания и проверки 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.
- 6.6.9.** Получать уведомления о выполняемых операциях с персональным ключом электронной подписи, хранение которого осуществляется с использованием СЭП.
- 6.6.10.** Применять одноразовый пароль, получаемый в SMS-сообщении на зарегистрированный Оператором УЦ номер мобильного телефона, для аутентификации при осуществлении доступа к СЭП и подтверждения применения персонального ключа электронной подписи, хранение которого осуществляется с использованием СЭП.
- 6.6.11.** Обратиться к Оператору УЦ для прекращения/приостановления действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи.
- 6.6.12.** Обратиться к Оператору УЦ центра для возобновления действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи и срока, на который действие сертификата было приостановлено.



7. Ответственность сторон и Разрешение споров.

7.1. 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.

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

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

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

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

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



8. Порядок предоставления и пользования услугами Удостоверяющего центра.

8.1. Регистрация Пользователей Оператором Удостоверяющего центра.

Оператор УЦ осуществляет регистрацию Пользователя в Удостоверяющем центре, создание и выдачу Сертификата ключа электронной подписи, только в том случае, если Сторона, полномочным представителем которой является регистрирующееся лицо, присоединилась к настоящему Регламенту путем предоставления Заявления и документов, подтверждающих сведения, необходимые для идентификации Пользователя УЦ предусмотренных разделом 5 настоящего Регламента.

8.1.1. Регистрация пользователей и создание первого сертификата ключа проверки электронной подписи.

Регистрация Пользователя в Удостоверяющем Центре осуществляется на основании *Заявления о присоединении к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО», регистрацию, создание и выдачу сертификата ключа проверки электронной подписи, при личном обращении регистрирующегося физического лица, в офис Уполномоченной организации.*

Форма заявления приведена в Приложении №1 к настоящему Регламенту.

По итогам осуществления процедуры идентификации лица, проходящего процедуру регистрации, путем установления личности 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 УЦ.

Заявление на регистрацию рассматривается Оператором УЦ в течение 1 (одного) часа с момента приема в обработку.

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

При принятии положительного решения, Оператор УЦ выполняет регистрационные действия по занесению информации в реестр Удостоверяющего центра, формирует запрос и подтверждает создание ключа электронной подписи и сертификата ключа проверки электронной подписи посредством Сервиса электронной подписи.

На основании указанной в Заявлении информации Оператор УЦ устанавливает *Кодовое слово* – любое секретное слово, число или их комбинация, указанное в Заявлении и используемое для дополнительной идентификации Пользователя УЦ в СЭП.

Копии сертификата ключа проверки электронной подписи на бумажном носителе (по форме определенной Приложением № 9 к настоящему Регламенту) формируются в двух экземплярах, заверяются собственноручной подписью лица, проходящего процедуру регистрации, а также печатью и подписью сотрудника Уполномоченной организации.

По окончании процедуры регистрации Пользователю УЦ выдаются:

- Информация о регистрации Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО», содержащая логин и временный пароль для доступа к СЭП, посредством подключенной Информационной системы Уполномоченной организации, и QR-код для активации ключа электронной подписи в мобильном приложении myDSS. Форма приведена в Приложении №10 к настоящему Регламенту.
- Копия сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе.



8.2. Изменение регистрационных данных Пользователя УЦ.

В случае изменения каких-либо 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 реестре Удостоверяющего центра, путем подачи заявления по форме, предусмотренной Приложением № 2 к настоящему Регламенту.

Внесение изменений в регистрационные данные Пользователя УЦ осуществляется Оператором УЦ на основании *Заявления на изменение регистрационных данных Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» (Приложение № 2)*.

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.

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

Форма заявления на изменение регистрационных данных Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» приведена в Приложении № 2 к настоящему Регламенту.

По итогам осуществления процедуры идентификации обратившегося лица, путем установления личности 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 УЦ.

Заявление на изменение регистрационных данных Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» рассматривается Оператором УЦ 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 УЦ 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.

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

Подача Пользователем УЦ заявления на изменение регистрационных данных Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» осуществляется с использованием Сервиса электронной подписи посредством подключенной к СЭП Информационной системы Уполномоченной Организации.

Заявление на изменение регистрационных данных Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» в электронной форме представляет собой электронный документ, с подписью на действующем ключе электронной подписи Пользователя УЦ.

Значения полей Subject, Key Usage, Extended Key Usage, содержащиеся в запросе на сертификат должны быть идентичны значениям этих полей в сертификате ключа проверки электронной подписи, соответствующего ключу электронной подписи Пользователя УЦ, которым сформирована электронная подпись в заявлении, предоставляемом при регистрации, создании и выдаче сертификата ключа проверки электронной подписи Пользователя УЦ.

После получения заявления Оператор УЦ проверяет корректность электронной подписи, которой подписано заявление, устанавливает его автора, сравнивает значения полей Subject, Key Usage, Extended Key Usage, содержащиеся 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 УЦ 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 УЦ принимает заявление и осуществляет внесение изменений и актуализацию регистрационных данных Пользователя в соответствии с предоставленными документами.

По итогам внесения изменений и актуализацию регистрационных данных Пользователя в соответствии с предоставленными документами, Пользователь УЦ, посредством подключенной к СЭП Информационной системы Уполномоченной Организации, получает электронный документ, подписанный Оператором УЦ и содержащий информацию о выданном сертификате.

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

8.3. 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 УЦ на основании Заявления на создание и выдачу сертификата ключа проверки электронной подписи.

Заявление на создание и выдачу сертификата ключа проверки электронной подписи 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.

8.3.1. Создание и выдача сертификата ключа проверки электронной подписи по заявлению, поданному в бумажной форме.



Форма *Заявления на создание и выдачу сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»* приведена в Приложении № 3 к настоящему Регламенту.

По итогам осуществления процедуры идентификации обратившегося лица, путем установления личности 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 УЦ.

Заявление на создание ключа электронной подписи и сертификата ключа проверки электронной подписи рассматривается Оператором УЦ в течение 1 (одного) часа с момента его поступления.

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

При принятии положительного решения, Оператор УЦ 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 (по форме, определенной Приложением № 9 к настоящему Регламенту, формируются в двух экземплярах, заверяются собственноручной подписью лица, проходящего процедуру регистрации, а также печатью и подписью Оператора УЦ.

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.

8.3.2. Создание и выдача сертификата ключа проверки электронной подписи по заявлению, поданному в электронной форме.

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

Заявления на создание и выдачу сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» в электронной форме представляет собой электронный документ формата PKCS#7, с подписью на действующем ключе электронной подписи Пользователя УЦ.

Значения полей Subject, Key Usage, Extended Key Usage, содержащиеся в запросе на сертификат должны быть идентичны значениям этих полей в сертификате ключа проверки электронной подписи, соответствующего ключу электронной подписи Пользователя УЦ, которым сформирована электронная подпись в заявлении на создание и выдачу сертификата ключа проверки электронной подписи Пользователя УЦ.

После получения заявления Оператор УЦ проверяет корректность электронной подписи заявления и устанавливает его автора, сравнивает значения полей Subject, Key Usage, Extended Key Usage, содержащиеся в запросе на сертификат, со значениями, указанными в сертификате ключа проверки электронной подписи автора настоящего заявления.

Срок рассмотрения заявления и создание сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день с момента получения заявления.

В случае отрицательного результата проведенных проверок, Оператор УЦ отклоняет заявление на создание сертификата ключа проверки электронной подписи 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 УЦ принимает заявление на создание сертификата ключа проверки электронной подписи и осуществляет подтверждение создания сертификата ключа проверки электронной подписи.

По итогам создания сертификата ключа проверки электронной подписи, Пользователь УЦ, посредством подключенной к СЭП Информационной системы Уполномоченной Организации, получает электронный документ, подписанный Оператором УЦ и содержащий информацию о выданном сертификате.

Для возможности использования вновь полученного сертификата ключа проверки электронной подписи, Пользователь УЦ обязан ознакомиться с информацией, содержащейся в сертификате. Подтверждение ознакомления с данной информацией, осуществляется посредством подписания Пользователем УЦ полученного электронного документа с использованием действующего сертификата ключа проверки электронной подписи.

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

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

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

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

8.4.1. 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 ООО «КРИПТО-ПРО»* 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.

Подача заявления и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на прекращение действия сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ о прекращении действия сертификата ключа проверки электронной подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору УЦ.

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.

8.4.2. 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.

Заявление на прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» в электронной форме представляет собой электронный документ формата PKCS#7. 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.

Запрос на прекращение действия сертификата ключа проверки электронной подписи представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер сертификата ключа проверки электронной подписи, действие которого прекращается;
- ReasonCode - код причины прекращения действия сертификата из следующего перечня допустимых значений:
 - "0" Не указана
 - "1" Компрометация ключа
 - "2" Компрометация ЦС
 - "3" Изменение принадлежности
 - "4" Сертификат заменен
 - "5" Прекращение работы
- SomeComment - текстовое значение комментария владельца сертификата ключа проверки электронной подписи (Пользователя УЦ).

После получения заявления Оператор УЦ 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.

Срок рассмотрения заявления на прекращение действия сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день с момента получения заявления Оператором УЦ.

В случае отрицательного результата проведенных проверок, Оператор УЦ отклоняет заявление на прекращение действия сертификата ключа проверки электронной подписи 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 УЦ прекращает действие сертификата ключа проверки электронной подписи и отправляет уведомление Пользователю УЦ.

Обработка заявления на прекращение действия сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ о прекращении действия сертификата ключа проверки электронной подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было получено заявление Оператором УЦ.

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 изданные Удостоверяющим центром сертификаты ключа подписи в поле `CRL Distribution Point` («Точка распространения списков отзыва»).

8.5. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ.

Для осуществления приостановления действия сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на приостановление действия сертификата ключа проверки электронной подписи.

Приостановление действия сертификата ключа подписи Пользователя УЦ осуществляется Оператором УЦ центра на основании заявления, поступающего в устной, бумажной или электронной форме.

Заявление в устной форме делается Оператору УЦ по телефону Уполномоченной организации.

Заявитель должен сообщить Оператору УЦ следующую информацию:

- Идентификационные данные владельца сертификата ключа проверки электронной подписи;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа проверки электронной подписи;
- кодовое слово Пользователя УЦ (указанное в Заявлении на регистрацию Пользователя УЦ).

Заявление принимается только в случае положительной аутентификации Пользователя УЦ (совпадения кодового слова, указанного в заявлении с информацией из реестра пользователей Удостоверяющего центра).

Заявление на приостановление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» в бумажной форме подается Оператору УЦ по форме, определенной Приложением № 5 и содержит следующую информацию:

- идентификационные данные владельца сертификата ключа проверки электронной подписи;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;

- срок, на который приостанавливается действие сертификата ключа проверки электронной подписи;
- дата и время подачи заявления.

Заявление на приостановление действия сертификата ключа проверки электронной подписи заверяется собственноручной подписью владельца сертификата (Пользователя УЦ) и подается в офисе Уполномоченной Организации при личном прибытии заявителя.

Заявление на приостановление действия сертификата ключа проверки электронной подписи в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на приостановление действия сертификата, а электронная подпись создается с применением действующего ключа электронной подписи Пользователя УЦ.

Заявление на приостановление действия сертификата ключа проверки электронной подписи в электронном виде формируется и подается Оператору УЦ с использованием Сервиса электронной подписи посредством подключенной к СЭП Информационной системы Уполномоченной Организации.

После получения отправленного заявления Оператор УЦ проверяет корректность электронной подписи заявления и определяет его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа проверки электронной подписи (сертификата, действие которого требуется приостановить), серийный номер которого указан в запросе на приостановление действия сертификата ключа проверки электронной подписи.

Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата составляет 10 (десять) дней.

Подача заявления на приостановление действия сертификата Оператору УЦ и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на приостановление действия сертификата ключа проверки электронной подписи и оповещение Пользователя УЦ о приостановлении действия сертификата должны быть осуществлены не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору УЦ.

Официальным уведомлением о приостановлении действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в создаваемые Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point («Точка распространения списков отзыва»).

В том случае, если Оператору УЦ в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователя УЦ не поступает заявление о возобновлении действия данного сертификата, его действие прекращается Удостоверяющим центром.

8.6. Возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

Для осуществления возобновления действия сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на возобновление действия сертификата.

Возобновление действия сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется Оператором УЦ на основании заявления на возобновление действия сертификата ключа проверки электронной подписи, поступающего в бумажной или электронной форме.

Заявление на возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» в бумажной форме подается в офисе Уполномоченной организации по форме, определенной Приложением № 6 и содержит следующую информацию:

- идентификационные данные владельца сертификата ключа проверки электронной подписи;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется возобновить;
- дата и время подачи заявления.

Заявление на возобновление действия сертификата ключа проверки электронной подписи, в бумажной форме заверяется собственноручной подписью владельца сертификата (Пользователя УЦ) и подается в офисе Уполномоченной организации при личном прибытии заявителя.

Заявление на возобновление действия сертификата ключа проверки электронной подписи в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на возобновление действия сертификата, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя УЦ.

Заявление на возобновление действия сертификата ключа проверки электронной подписи формируется и подается в электронном виде в Оператору УЦ центра с использованием Сервиса электронной подписи посредством подключенной к СЭП Информационной системы Уполномоченной Организации.

После получения отправленного заявления Оператор УЦ проверяет корректность электронной подписи заявления и определяет его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа проверки электронной подписи (сертификата, действие которого требуется возобновить), серийный номер которого указан в запросе на возобновление действия сертификата ключа проверки электронной подписи.

Подача заявления на возобновление действия сертификата Оператору УЦ и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на возобновление действия сертификата и оповещение Пользователя УЦ о возобновлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору УЦ.

Официальным уведомлением о возобновлении действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в создаваемые Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point («Точка распространения списков отзыва»).

8.7. Подтверждение подлинности ЭП в электронном документе.

Для подтверждения подлинности электронной подписи в электронных документах, циркулирующих в Информационной системе, Пользователь УЦ подает Заявление на подтверждение подлинности ЭП в электронном документе Оператору УЦ в офисе Уполномоченной организации.

Подтверждение подлинности ЭП электронного документа осуществляется на основании *Заявления на подтверждение подлинности электронной подписи в электронном документе* в бумажной форме, определенной Приложением № 7 настоящего Регламента и содержащего следующую информацию:

- Дата и время подачи заявления;
- Идентификационные данные Пользователя УЦ, ЭП которого требуется проверить в электронном документе;
- Серийный номер сертификата ключа проверки электронной подписи, на котором требуется проверить ЭП электронного документа;
- дата и время формирования ЭП в электронном документе.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является файл на сменном USB или CD (DVD) носителе, содержащий электронный документ.

Предоставляемый файл получается путем экспорта электронного документа, к которому применена электронная подпись, из Информационной системы.

Электронная подпись в предоставленном электронном документе будет считаться равнозначной собственноручной подписи при выполнении следующих условий:

- сертификат ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, не утратил силу (действует) на момент формирования ЭП в электронном;
- электронная подпись, проверенная на сертификате ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, верна;
- формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

Срок проведения работ по заявлению на подтверждение подлинности ЭП в электронном документе и предоставлению заключения о произведенной проверке составляет 15 (пятнадцать) рабочих дней с момента его предоставления Оператору УЦ.

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа работников Уполномоченной организации. При проведении указанных работ Уполномоченная организация (комиссия) имеет право привлекать к проведению экспертных работ работников Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение в письменной форме, подписанное всеми членами комиссии и заверенное печатью Уполномоченной организации.

Заключение содержит:

- результат проверки ЭП электронного документа;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные комиссии для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

8.8. Подтверждение подлинности электронной подписи Удостоверяющего центра в созданных Сертификатах.

Для подтверждения подлинности электронной подписи Удостоверяющего центра в сертификате ключа проверки электронной подписи Пользователь УЦ подает *Заявление на подтверждение подлинности электронной подписи Удостоверяющего центра в сертификате ключа проверки электронной подписи* Оператору Удостоверяющего центра по форме, определенной Приложением № 8.

Заявление должно содержать следующую информацию:

- Дата и время подачи заявления;
- Идентификационные данные субъекта, в сертификате ключа проверки электронной подписи которого необходимо подтвердить электронную подпись Удостоверяющего центра;
- Серийный номер сертификата ключа проверки электронной подписи, в котором необходимо подтвердить электронную подпись Удостоверяющего центра.

Обязательным приложением к заявлению на подтверждение подлинности электронной подписи Удостоверяющего центра в сертификате ключа проверки электронной подписи является сменный USB или CD (DVD) носитель, содержащий файл проверяемого сертификата ключа проверки электронной подписи.

Срок проведения работ по подтверждению подлинности ЭП и предоставлению заключения о произведенной проверке составляет 15 (Пятнадцать) рабочих дней с момента его предоставления Оператору Удостоверяющего центра.

На основании полученного заявления Оператор УЦ установленным порядком обращается в Удостоверяющий центр, который осуществляет подтверждение подлинности электронной подписи Удостоверяющего центра в сертификате ключа проверки электронной подписи.

Результатом проведения работ по подтверждению подлинности электронной подписи Удостоверяющего центра в сертификате ключа проверки электронной подписи является заключение Удостоверяющего центра в письменной форме, подписанное уполномоченным лицом Удостоверяющего центра и заверенное печатью Удостоверяющего центра.

Заключение содержит:

- результат проверки электронной подписи Удостоверяющего Центра;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;



- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме.

8.9. 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.

Удостоверяющий центр предоставляет актуальную информацию 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://qs.cryptopro.ru/ocspkc3/ocsp.srf>. Указанный адрес заносится в расширение «[1]Доступ к сведениям центра сертификации - Метод доступа=Протокол определения

состояния сертификата через сеть (1.3.6.1.5.5.7.48.1)», издаваемых УЦ 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>.

8.10. 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.



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

9.1. Форма сертификатов ключа проверки электронной подписи, выдаваемых Уполномоченной организацией.

Форма сертификатов ключей проверки электронной подписи, выдаваемых Уполномоченной организацией, 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 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. Форма списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reason Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы



		"6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
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 Удостоверяющего Центра

9.3. Сроки действия ключевых документов.

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

Срок действия ключа электронной подписи Пользователя УЦ составляет 1 (один) год.

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

Срок действия сертификата ключа проверки электронной подписи Пользователя УЦ не превышает 1 (один) год. Время начала периода действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.



10. Дополнительные положения.

10.1. Плановая смена ключа 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.

Старый ключ электронной подписи Удостоверяющего центра используется для формирования списков отозванных сертификатов, изданных 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 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.

10.3. Компрометация ключевых документов Пользователя Удостоверяющего центра.

Пользователь УЦ самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи.

В случае компрометации или угрозы компрометации ключа электронной подписи Пользователь УЦ связывается с Оператором УЦ по телефону и сообщает ему следующие сведения:

- Свои идентификационные данные;

- Серийный номер сертификата ключа проверки электронной подписи, соответствующего скомпрометированному ключу (по возможности);
- Кодовое слово, указанное при регистрации.

Оператор УЦ производит идентификацию Пользователя УЦ по кодовому слову.

В случае успешной аутентификации Оператор УЦ приостанавливает действие сертификата на 30 (тридцать) календарных дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователь не направит Оператору УЦ заявление на возобновление действия сертификата, то Удостоверяющий центр автоматически прекращает действие данного сертификата.

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 8.3 настоящего Регламента.

10.4. Конфиденциальность информации.

10.4.1. 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.

10.4.2. 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.

10.4.3. 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.

10.5. Форс-мажор.

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

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

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

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

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

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



11. Список приложений.

Приложение №1. Форма Заявления о присоединении к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО», регистрацию, создание и выдачу сертификата ключа проверки электронной подписи.

Приложение №2. Форма Заявления на изменение регистрационных данных Пользователя в реестре Удостоверяющего центра ООО «КРИПТО-ПРО».

Приложение №3. Форма заявления на создание и выдачу сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

Приложение №4. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

Приложение №5. Форма заявления на приостановление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

Приложение №6. Форма заявления на возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

Приложение №7. Форма заявления на подтверждение подлинности электронной подписи в электронном документе.

Приложение №8. Форма заявления на подтверждение подлинности электронной подписи в сертификате ключа проверки электронной подписи.

Приложение №9. Форма копии сертификата ключа проверки электронной подписи Пользователя (Пример).

Приложение №10. Информация о регистрации Пользователя в Удостоверяющем центре (Пример).

Приложение №11. Реализуемые функции Сервиса электронной подписи.



Приложение №1 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО».
Форма Заявления о присоединении к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»,
регистрацию, создание и выдачу сертификата ключа проверки электронной подписи

**Заявление о присоединении к Регламенту
Уполномоченной организации УЦ ООО «КРИПТО-ПРО»,
регистрацию, создание и выдачу сертификата ключа проверки
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 Удостоверяющего центра ООО «КРИПТО-ПРО» по выдаче и управлению квалифицированными сертификатами ключей проверки электронной подписи, предоставлению доступа к Сервису электронной подписи (далее Регламент). С настоящим Регламентом и приложениями к нему ознакомлен и являюсь Стороной Регламента с момента подписания настоящего Заявления

Прошу зарегистрировать и создать сертификат ключа проверки электронной подписи в **Реестре Удостоверяющего центра ООО «КРИПТО-ПРО»** 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 Удостоверяющего центра ООО «КРИПТО-ПРО», установленными Регламентом Уполномоченной организации Удостоверяющего центра ООО «КРИПТО-ПРО».

Настоящим выражаю согласие с обработкой Удостоверяющим центром ООО «КРИПТО-ПРО» и Уполномоченной организацией своих персональных данных и признаю, что персональные данные, заносимые в сертификаты ключей проверки

¹ Указывается только для индивидуальных предпринимателей



электронной подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным.

Поручаю Удостоверяющему центру ООО «КРИПТО-ПРО» хранение ключей электронной подписи, созданных с использованием Сервиса электронной подписи, подписания с их помощью электронных документов и передачи подписанных электронных документов Уполномоченной организации по моим волеизъявлениям в установленном правилами работы Сервиса электронной подписи порядке.

Подтверждаю, что с правилами работы Сервиса электронной подписи ознакомлен(-а), его положения мне известны, понятны и мной осознаны, возникающие из них и в соответствии с ними обязательства, 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 Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма Заявления на изменение регистрационных данных Пользователя в реестре
Удостоверяющего центра ООО «КРИПТО-ПРО»

Заявление на изменение регистрационных данных Пользователя в реестре Удостоверяющего центра ООО «КРИПТО-ПРО»

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

(серия и номер паспорта, кем и когда выдан)

Прошу внести изменения в информацию, содержащуюся в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО» 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 Удостоверяющим центром ООО «КРИПТО-ПРО» 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.

С Регламентом Уполномоченной организации Удостоверяющего центра ООО «КРИПТО-ПРО» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Подтверждаю, что с правилами работы Сервиса электронной подписи ознакомлен(-а), его положения мне известны, понятны и мной осознаны, возникающие из них и в соответствии с ними обязательства, требования и обязанности признаю, принимаю и обязуюсь исполнять надлежащим образом.

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

² Указывается только для индивидуальных предпринимателей



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 №3 к Регламенту Уполномоченной Организации УЦ ООО «КРИПТО-ПРО»
Форма заявления на создание и выдачу сертификата ключа проверки электронной
подписи Пользователя УЦ ООО «КРИПТО-ПРО»

**Заявление на создание и выдачу сертификата ключа проверки
электронной подписи Пользователя Удостоверяющего центра ООО
«КРИПТО-ПРО»**

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

(серия и номер паспорта, кем и когда выдан)

Прошу создать сертификат ключа проверки 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 ³	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

_____/_____
(подпись) (фамилия, инициалы)

«_____» _____ 20__ года
(дата)

³ Указывается только для индивидуальных предпринимателей



Приложение №4 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма заявления на прекращение действия сертификата ключа проверки
электронной подписи Пользователя УЦ «КРИПТО-ПРО»

**Заявление на прекращение действия сертификата ключа проверки
электронной подписи Пользователя Удостоверяющего центра
ООО «КРИПТО-ПРО»**

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

(серия и номер паспорта, кем и когда выдан)

В СВЯЗИ С _____
(причина отзыва сертификата)

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

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 ⁴	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

Подпись Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____/_____
(подпись) (фамилия, инициалы)

« _____ » _____ 20__ года
(дата)

⁴ Указывается только для индивидуальных предпринимателей



Приложение №5 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма заявления на приостановление действия сертификата ключа проверки
электронной подписи Пользователя УЦ «КРИПТО-ПРО»

**Заявление на приостановление действия сертификата ключа проверки
электронной подписи Пользователя Удостоверяющего центра
ООО «КРИПТО-ПРО»**

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

(серия и номер паспорта, кем и когда выдан)

В СВЯЗИ С _____
(причина отзыва сертификата)

Прошу приостановить действие моего сертификата ключа проверки электронной подписи»,
содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата	
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 ⁵	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Время и дата предоставления Заявления
"_____:_____" "____/____/____"
Час/минута день/ месяц/год

Подпись Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

(подпись) (фамилия, инициалы)
«____» _____ 20__ года
(дата)

⁵ Указывается только для индивидуальных предпринимателей



Приложение №6 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма заявления на возобновление действия сертификата ключа проверки электронной
подписи Пользователя УЦ «КРИПТО-ПРО»

**Заявление на возобновление действия сертификата ключа проверки
электронной подписи Пользователя Удостоверяющего центра
ООО «КРИПТО-ПРО»**

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

(серия и номер паспорта, кем и когда выдан)

Прошу возобновить действие моего сертификата ключа проверки электронной подписи»,
содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата	
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 ⁶	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

Время и дата предоставления Заявления
"_____:_____" "____/____/____"
Час/минута день/ месяц/год

Подпись Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

(подпись) (фамилия, инициалы)
«____» _____ 20__ года
(дата)

⁶ Указывается только для индивидуальных предпринимателей



Приложение №7 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма заявления на подтверждение электронной подписи в электронном документе

**Заявление на подтверждение подлинности электронной подписи в
электронном документе**

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

(серия и номер паспорта, кем и когда выдан)

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

SerialNumber (SN)	Серийный номер сертификата	
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 ⁷	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

Файл, созданный с использованием СЭП, содержащий подписанные ЭП данные и значения ЭП, либо файл,
содержащий исходные данные и файл, содержащий значение ЭП формата CMS, на прилагаемом к
заявлению носителе с указанием рег № ДД.ММ.ГГГГ

Время и дата формирования ЭП в электронном документе

"____:____" "____/____/____"

Час/минута день/ месяц/год

Время и дата предоставления Заявления

"____:____" "____/____/____"

Час/минута день/ месяц/год

Подпись Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____/_____/____/

«____» _____ 20____ г.

⁷ Указывается только для индивидуальных предпринимателей



Приложение №8 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма заявления на подтверждение подлинности электронной подписи
Удостоверяющего центра в сертификате ключа проверки электронной подписи

**Заявление на подтверждение подлинности электронной подписи
Удостоверяющего центра в сертификате ключа проверки
электронной подписи**

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

(серия и номер паспорта, кем и когда выдан)

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

SerialNumber (SN)	Серийный номер сертификата	
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 ⁸	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) заявителя	

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 с указанием рег № ДД.ММ.ГГГГ

Время на момент наступления которого требуется подтвердить подлинность ЭП

"____:____" ____/____/____
Час/минута день/ месяц/год

Время и дата предоставления Заявления

"____:____" ____/____/____
Час/минута день/ месяц/год

Подпись Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____/_____
« ____ » _____ 20 ____ г.

⁸ Указывается только для индивидуальных предпринимателей



Регламент Уполномоченной организации по выдаче и управлению
квалифицированными сертификатами ключей проверки электронной подписи
Пользователей Удостоверяющего центра "КРИПТО-ПРО"

Приложение №9 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Форма копии сертификата ключа проверки электронной подписи Пользователя
Удостоверяющего центра ООО «КРИПТО-ПРО»

Копия сертификата ключа проверки электронной подписи

Сведения о сертификате:

Кому выдан:

Петров Пётр Петрович

Версия: 3 (0x2)

Серийный номер: 61D0 B15A 0007 0000 007A

Издатель сертификата: CN = ООО «КРИПТО-ПРО», O = ООО "КРИПТО-ПРО", L = Москва, S = г. Москва, C = RU, E = qsa@cryptopro.ru, STREET = ул. Суцёвский 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, CN = Петров Пётр Петрович, STREET = Курортный пр-т, дом 25, L = Сочи, S = 23 Краснодарский край, C = RU, E = petrov@sochi.ru, SNILS = 5222222222

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 = qsa@cryptopro.ru, STREET = ул. Суцёвский 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 распространения 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 KC1 [2]Политика сертификата:

Идентификатор политики=Класс средства ЭП KC2

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: _____/_____

"__" _____ 20__ г.

Подпись Оператора Удостоверяющего центра: _____/_____

"__" _____ 20__ г.

МП



Приложение № 10 к Регламенту Уполномоченной организации УЦ ООО «КРИПТО-ПРО»
Информация о регистрации Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО»

Информация о регистрации Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО»

На основании предоставленного Заявления на регистрацию Пользователя в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО» 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 myDSS	

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

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

Сохранность и неразглашение полученного логина/пароля обеспечивается Пользователем.

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



Реализуемые функции Сервиса электронной подписи ООО «КРИПТО-ПРО»

1. Назначение сервиса

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

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

2. Поддерживаемые форматы и стандарты

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

Поддерживаемые форматы криптографических сообщений:

1. Электронная подпись ГОСТ 34.10–2012;
2. Усовершенствованная подпись в соответствии с ETSI TS 101 733 "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (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 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, и (или) подключенной к СЭП Информационной системы Уполномоченной Организации.



Первичная аутентификация Пользователей УЦ для управления доступом к СЭП осуществляется средствами Уполномоченной организации. Вторичная аутентификация Пользователей УЦ для подтверждения использования ключа электронной подписи осуществляется посредством одноразового кода, формируемого и проверяемого СЭП и высылаемого Пользователям УЦ в SMS-сообщении через оператора сотовой связи посредством SMS-шлюза Уполномоченной организации.

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

5. Информирование пользователей

Сервис электронной подписи позволяет информировать Пользователей УЦ посредством отправки через оператора сотовой связи посредством SMS-шлюза Уполномоченной организации SMS-сообщений, содержащих сведения о подключении к СЭП и подписываемых электронных документах от имени Пользователя УЦ, выполняемых операциях с ключом электронной подписи, принадлежащих Пользователю УЦ.

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, 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.

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

Создание сертификата ключа проверки электронной подписи для использования в СЭП осуществляется подключенным к СЭП Удостоверяющим центром ООО «КРИПТО-ПРО».

Использование ключа электронной подписи в СЭП должно подтверждаться владельцем соответствующего сертификата ключа проверки электронной подписи (Пользователем УЦ) с помощью одноразового кода, высылаемого в SMS-сообщении на указанный при регистрации мобильный телефон владельца сертификата (Пользователя



УЦ), а также индивидуальным PIN-кодом доступа к ключевому контейнеру, содержащему используемый ключ электронной подписи.

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

Пользователь УЦ обязан немедленно обратиться к Оператору УЦ 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 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.*

На рабочих местах Пользователей УЦ должны использоваться сертифицированные средства антивирусной защиты.