«УТВЕРЖДАЮ»
И.О. генерального директора
ООО «КОРУС Консалтинг СНГ»

_____Тарасов В.Г.

«27» декабря 2023

Регламент
Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»
по созданию и управлению сертификатами ключей проверки электронной подписи, используемыми для создания усиленной неквалифицированной электронной подписи

г. Санкт-Петербург
2023г.

СОДЕРЖАНИЕ

1. Основные понятия

В деятельности Удостоверяющего центра ООО «КОРУС Консалтинг СНГ» используются основные понятия в значениях, указанных в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» и в настоящем Регламенте:

Сертификат ключа проверки электронной подписи (далее – СКПЭП) – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи

Список отозванных сертификатов (далее – СОС) – файл в формате crl, содержащий в себе серийные номера аннулированных СКПЭП и СКПЭП, прекративших свое действие до истечения установленного срока его действия.

Отзыв СКПЭП – операция УЦ, направленная на аннулирование или прекращение действия СКПЭП, до истечения установленного срока его действия, влекущая за собой включение в СОС серийного номера этого СКПЭП.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Вручение сертификата ключа проверки электронной подписи – передача сотрудником/доверенным лицом Удостоверяющего центра изготовленного этим Удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Доверенное лицо Удостоверяющего центра – физическое или юридическое лицо (в лице физического лица), наделенное полномочиями по установлению личности Заявителя, проверке и приему документов, вручению сертификатов ключей проверки электронной подписи.

Заявитель Удостоверяющего центра – физическое лицо (в случае присоединения к настоящему Регламенту юридического лица или индивидуального предпринимателя – физическое лицо, являющееся уполномоченным представителем юридического лица, индивидуального предпринимателя), присоединившееся к настоящему Регламенту.

Усиленная неквалифицированная электронная подпись (далее – НЭП) - электронная подпись, соответствующая следующим признакам:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- создается с использованием средств электронной подписи.

Клиент Удостоверяющего центра – юридическое лицо, индивидуальный предприниматель или физическое лицо, обратившееся в Удостоверяющий центр за услугой по изготовлению СКПЭП и/или за получением прямо связанных с этим иных услуг и прав (лицензий) на ПО.

Субъекты – это все лица, которые в силу настоящего Регламента, договора или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Регламентом. Субъектами, на которых распространяется действие настоящего Регламента, являются – Клиент УЦ, Заявитель УЦ, Владелец СКПЭП, и/или Удостоверяющий центр (если соответствует смысловой нагрузки соответствующего условия).

Ключевой носитель – аппаратное или программно-аппаратное устройство хранения ключей ЭП, являющееся персональным средством, обеспечивающим защиту хранения ключей ЭП.

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

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

Компрометация ключа подписи – нарушение конфиденциальности или подозрение в нарушении конфиденциальности ключа электронной подписи.

Доверенная информационная система – любая информационная система (программа для ЭВМ), участниками которой может быть ограниченный круг лиц, определенный ее оператором или соглашением участников этой информационной системы, и в которой работает и/или планирует работать Заявитель/Клиент УЦ.

Корректная (подлинная) электронная подпись – электронная подпись, проверка которой с помощью средства электронной подписи и с использованием сертификата ключа подписи, действующего на момент создания подписи, дала положительный результат.

Некорректная (неподлинная) электронная подпись – электронная подпись, проверка которой с помощью средства электронной подписи и с использованием сертификата ключа подписи, действующего на момент создания подписи, дала отрицательный результат.

Простая электронная подпись (далее – ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Для создания ПЭП используется ключ ПЭП – сочетание идентификатора и пароля (кода). Допустимые форматы ключа ПЭП, а также случаи и порядок использования ПЭП определяются настоящим Регламентом.

Сотрудник Удостоверяющего центра - уполномоченное лицо Удостоверяющего центра, наделенное Удостоверяющим центром полномочиями по осуществлению действий по созданию, регистрации и управлению СКПЭП владельцев сертификата Удостоверяющего центра, а также иными полномочиями согласно настоящего Регламента.

Средство криптографической защиты информации (СКЗИ):

- программное, аппаратное или аппаратно-программное средство, реализующее криптографические алгоритмы преобразования данных и предназначенное для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи;
- программное, аппаратное или аппаратно-программное средство, реализующее криптографические алгоритмы преобразования данных и предназначенное для защиты информации от искажения информации и навязывания ложной информации;
- программное, аппаратное или аппаратно-программное средство, предназначенное для изготовления и распределения криптографических ключей.

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.

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

2. Общие положения

2.1. Предмет регулирования Регламента:

Настоящий Регламент учитывает положения действующего законодательства Российской Федерации, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», является руководящим документом Удостоверяющего центра ООО «КОРУС Консалтинг СНГ» (далее – Удостоверяющий центр, УЦ) и устанавливает общий порядок и условия предоставления Удостоверяющим центром услуг по созданию и управлению СКПЭП, используемыми для создания НЭП и оказанию дополнительных услуг.

2.2. Сведения об Удостоверяющем центре:

2.2.1. Удостоверяющий центр осуществляет целевые функции по созданию и выдаче сертификатов ключа проверки электронной подписи и иные функции удостоверяющего центра

в соответствии с требованиями действующей редакции Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами.

2.2.2. УЦ осуществляет свою деятельность на территории Российской Федерации в качестве профессионального участника рынка на основании лицензии Управления Федеральной службы безопасности Российской Федерации по г.Санкт-Петербургу и Ленинградской области, размещенной в сети «Интернет» по адресу: www.esphere.ru в разделе «О компании».

2.2.3. Контактные реквизиты Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:
Полное наименование: Общество с ограниченной ответственностью «КОРУС Консалтинг СНГ».
Юридический адрес: 194100, г. Санкт-Петербург, Б. Сампсониевский пр-кт, д.68, лит.Н, пом.1Н.
Местонахождение Удостоверяющего центра: 194100, г.Санкт-Петербург, Б. Сампсониевский пр-т, д.68, лит.Н, пом.1Н
ИНН 7801392271
ОГРН 1057812752502
Контактный телефон: 8 (800) 100-8-812
Адрес электронной почты: help@esphere.ru
Сайт ООО «КОРУС Консалтинг СНГ»: www.esphere.ru
Адреса офисов Удостоверяющего центра опубликованы на сайте https://www.esphere.ru/products/uc/
Рабочий день офисов Удостоверяющего центра (далее – рабочий день) – промежуток времени с 09:00 по 18:00 (МСК.) каждого рабочего дня недели, за исключением выходных и праздничных дней.
Создание и вручение сертификатов в офисах УЦ осуществляется в рабочие дни.
Создание и вручение сертификатов вне офисов УЦ осуществляется в течение 24 часов в сутки с даты принятия заявления на изготовление СКПЭП (п.5.3 Регламента), 7 дней в неделю, 365 (366 для високосного года) дней в году.

2.3. Действующая редакция Регламента размещена в сети Интернет по адресу www.esphere.ru, в разделе «Удостоверяющий центр».

2.4. Информирование потенциальных Субъектов по вопросам предоставления услуг Удостоверяющим центром производится по контактным телефонам, адресу электронной почты, в офисах УЦ в рабочие дни, указанным в п.2.2.3 Регламента.

Информирование текущих Субъектов по вопросам предоставления услуг Удостоверяющим центром производится либо посредством направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром, либо посредством направления SMS-уведомлений на телефонный номер, представленный Заявителем УЦ и/или Владельцем СКПЭП в Удостоверяющий центр, и/или посредством размещения информации на сайте по адресу https://www.esphere.ru/products/uc/, или сочетание таких способов.

2.5. Присоединение Заявителя УЦ/Клиента УЦ/Владельца СКПЭП к настоящему Регламенту и оказание таким лицам услуг, предусмотренных настоящим Регламентом, осуществляется либо путем подписания двустороннего договора, либо путем представления заявления на заключение договора и присоединение к Условиям о предоставлении услуг и иных обязательств ООО «КОРУС Консалтинг СНГ», либо путем представления (подписания) заявления на изготовление СКПЭП, в т.ч. электронной подписью, либо путем оплаты счета, оформленного согласно Договора (Оферты) на оказание услуг удостоверяющего центра, или выражением волеизъявления на его оплату. При использовании Субъектом доверенной информационной системы для создания и получения СКП ЭП, присоединяясь к настоящему Регламенту, Субъект подтверждает своё ознакомление с руководством пользователя доверенной информационной системы при работе в ней.

Факт присоединения Субъекта к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент подачи присоединения к нему одним из вышеописанных способов. Субъект, присоединившийся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями п.2.7 настоящего Регламента.

2.6. Изготовление СКПЭП осуществляется на возмездной основе, если в договоре предоставления услуг не указано иное, на основании заявления на изготовление такого сертификата, оформленного Клиентом, и документов, на основании которых Удостоверяющим центром вносятся сведения в СКПЭП. Форма заявления направляется клиенту в доверенной информационной системе или посредством контактного адреса электронной почты.

2.7. Внесение изменений в настоящий Регламент, включая приложения к нему, производится УЦ в одностороннем порядке путем опубликования новой редакции Регламента на официальном сайте ООО «КОРУС Консалтинг СНГ» по адресу: www.esphere.ru в разделе «Удостоверяющий центр».

Любые изменения, вносимые в настоящий Регламент, с момента вступления в силу равно распространяются на всех лиц, присоединившихся к настоящему Регламенту, в том числе присоединившихся к настоящему Регламенту ранее даты вступления изменений в силу.

Субъект, присоединившийся к Регламенту, вправе в любое время, в том числе в случае несогласия с изменениями (дополнениями), внесенными Удостоверяющим центром в Регламент, в одностороннем внесудебном порядке отказаться от исполнения Регламента путем предоставления в Удостоверяющий центр уведомления. Указанное уведомление должно быть оформлено в письменной форме и направлено в Удостоверяющий центр способом, позволяющим достоверно установить факт его получения Удостоверяющим центром. Данное письменное уведомление, полученное Удостоверяющим центром, является основанием для обязательного досрочного прекращения действия СКПЭП лица, предоставившего уведомление об отказе от исполнения Регламента, в порядке, установленном настоящим Регламентом и Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи». После получения указанного уведомления Удостоверяющим центром на лицо, предоставившее данное уведомление, действие Регламента не распространяется.

2.8. Удостоверяющий центр вправе в одностороннем внесудебном порядке отказаться от исполнения настоящего Регламента в случае нарушения Субъектом, присоединившимся к Регламенту, условий настоящего Регламента. Отказ от исполнения Регламента не влияет на действительность электронных подписей Субъекта, присоединившегося к Регламенту, созданных до даты такого отказа.

2.9. Выполнение ООО «КОРУС Консалтинг СНГ» функций Удостоверяющего центра может быть прекращено в порядке, установленном законодательством Российской Федерации, и на основании локально-нормативных актов ООО «КОРУС Консалтинг СНГ».

3. Перечень реализуемых Удостоверяющим центром функций

3.1. Создание и выдача СКПЭП в соответствии с требованиями, указанными в Федеральном законе № 63-ФЗ от 06.04.2011 «Об электронной подписи».

3.2. Осуществление в соответствии с правилами подтверждения владения ключом электронной подписи, описанного в п. 5.1.2. настоящего Регламента, подтверждения владения получателем сертификата ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата.

3.3. Установление сроков действия СКПЭП.

3.4. Отзыв СКПЭП в виде аннулирования СКПЭП или прекращения действия СКПЭП, до истечения установленного его срока, выданных Удостоверяющим центром.

3.5. Выдача средств электронной подписи, содержащих ключ электронной подписи и ключ проверки электронной подписи или обеспечивающих возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем УЦ.

3.6. Предоставление прав использования программ (лицензий), необходимых для использования/управления СКПЭП в электронно-вычислительных машинах и доверенных информационных системах.

3.7. Ведение реестров выданных Удостоверяющим центром СКПЭП, аннулированных или прекративших действие СКПЭП, до истечения установленного срока его действия, в том числе

включающего в себя информацию, содержащуюся в выданных этим УЦ СКПЭП, и информацию о датах прекращения действия СКПЭП и об основаниях таких прекращений действия.

3.8. Создание ключей электронной подписи и ключей проверки электронной подписи по обращению Заявителей УЦ.

3.9. Проверка уникальности ключей проверки электронной подписи в реестре сертификатов.

3.10. Осуществление проверки электронных подписей электронных документов на подлинность (корректность) по обращению участников электронного взаимодействия и/или предоставление информации о статусе сертификата ключа проверки электронной подписи в порядке, предусмотренном в п.5.3 настоящего Регламента.

3.11. Осуществление иной связанной с использованием средств электронной подписи деятельности.

4. Права и обязанности Субъектов

4.1. Удостоверяющий центр обязан:

4.1.1. Создать ключ электронной подписи, ключ проверки электронной подписи, СКПЭП на основании оформленного заявления на изготовление СКПЭП в соответствии с требованиями к заявлению, указанными в п. 5.5.2 Регламента, и порядком, определенным в настоящем Регламенте.

4.1.2. Вносить в создаваемые СКПЭП только достоверную и актуальную информацию, подтвержденную соответствующими документами и/или сведениями (информацией). Выдавать СКПЭП владельцу СКПЭП в форме электронного документа или на бумажном носителе.

4.1.3. Использовать ключ электронной подписи УЦ только для заверения создаваемых им (УЦ) СКПЭП, а также для заверения СОС.

4.1.4. Принять меры по защите ключа электронной подписи УЦ от несанкционированного доступа.

4.1.5. Организовать свою работу по московскому времени. УЦ синхронизирует все свои программные и технические средства обеспечения деятельности.

4.1.6. Обеспечить уникальность серийных номеров создаваемых СКПЭП.

4.1.7. Обеспечить уникальность значений ключей проверки электронной подписи в созданных СКПЭП.

4.1.8. Обеспечить конфиденциальность созданных удостоверяющих центром ключей электронной подписи.

4.1.9. Уведомить об отзыве СКПЭП всех лиц, зарегистрированных в УЦ, посредством публикации СОС, ссылка на который размещена в каждом СКПЭП.

Период публикации актуального СОС – не более 12 часов.

4.1.10. Обеспечивать круглосуточную доступность реестра сертификатов в информационно-телекоммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

4.1.11. Обеспечить актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

4.1.12. Отказать заявителю в создании СКПЭП в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата.

4.1.13. Отказать заявителю в создании СКПЭП в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата.

4.1.14. Отказать заявителю в создании СКПЭП в случае, отсутствия необходимого пакета документов и сведений, предусмотренных Приложением № 1 к Регламенту,

4.1.15. Отказать в изготовлении СКПЭП Заявителю при расхождении данных, предоставленных Заявителем с данными, указанными в ЕГРЮЛ или ЕГРИП.

4.1.16. Отказать в изготовлении СКПЭП Заявителю, если в ЕГРЮЛ или ЕГРИП содержится отметка о недостоверности каких-либо сведений.

4.1.17. Строго соблюдать срок использования ключей электронной подписи УЦ в соответствии с правилами использования СКЗИ, а также с учетом того, чтобы по окончанию сроков действия, соответствующих им СКПЭП, все подписанные этими ключами сертификаты пользователей и СОС уже прекратили свое действие.

4.1.18. Осуществлять иные действия по реализации прав, предоставленных Заявителю УЦ и/или владельцу СКПЭП или третьему лицу настоящим Регламентом и/или законодательством Российской Федерации.

4.2. Сторона, присоединяющаяся к настоящему Регламенту, обязана:

4.2.1. Представить Удостоверяющему Центру документы, либо их надлежащим образом заверенные копии и сведения, содержащиеся в заявлении на изготовление СКПЭП и подлежащие включению Удостоверяющим центром в СКПЭП. Перечни и порядок предоставления соответствующих документов приведены в Приложении № 1 к настоящему Регламенту.

4.2.2. При получении СКПЭП ознакомиться с информацией, содержащейся в СКПЭП, собственноручно или способом, определенным в доверенной информационной системе, если иное не прописано в соглашении между участниками электронного взаимодействия.

4.2.3. Безусловно соблюдать положения настоящего Регламента.

4.3. Владелец СКПЭП обязан:

4.3.1. Хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его компрометации (т.е. потери, раскрытия, искажения и несанкционированного использования).

4.3.2. Применять для формирования электронной подписи только ключ, соответствующий действующему СКПЭП.

4.3.3. Не применять ключ электронной подписи, если есть основания полагать, что конфиденциальность данного ключа нарушена.

4.3.4. Немедленно обратиться в УЦ с заявлением на прекращение действия СКПЭП (Приложение № 4 к настоящему Регламенту) в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

4.3.5. Не использовать ключ электронной подписи, связанный с СКПЭП, заявление на прекращение действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в УЦ до момента официального уведомления Удостоверяющим центром о досрочном прекращении действия сертификата (до истечения установленного срока его действия), либо об отказе в прекращении действия.

4.3.6. Не использовать ключ электронной подписи, связанный с СКПЭП, действие которого прекращено.

4.4. Удостоверяющий центр имеет право:

4.4.1. Запрашивать у Заявителя УЦ документы и/или сведения для подтверждения любой содержащейся в заявлении на изготовление СКПЭП информации.

4.4.2. Не принимать от Заявителя УЦ документы и/или сведения, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации.

4.4.3. Без заявления владельца СКПЭП на прекращение СКПЭП прекратить срок действия СКПЭП до истечения срока его действия:

- в случае наличия у УЦ достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата;
- невыполнения владельцем СКПЭП обязанностей, установленных законодательством Российской Федерации в области электронной подписи;
- в случае появления у УЦ достоверных сведений о том, что документы и/или сведения, предоставленные Заявителем УЦ в целях создания и получения им сертификата, не

являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный сертификат;

- в случае отсутствия оплаты за услугу по созданию и выдаче данного сертификата в сроки и в порядке, описанные в договоре, заключенном между УЦ и Клиентом УЦ;
- в случае обнаружения в СКПЭП «опечатки» в сведениях, вносимых в сертификат.
- в случае одностороннего внесудебного отказа Заявителя УЦ/Клиента УЦ/Владельца СКПЭП от исполнения настоящего Регламента путем предоставления в Удостоверяющий центр соответствующего уведомления (п.2.8 Регламента);
- в иных случаях, установленных Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Субъектами.

4.4.4. Отказать в прекращении срока действия СКПЭП в случае ненадлежащего оформления соответствующего заявления (Приложение № 2 к настоящему Регламенту).

4.4.5. Осуществить проверку подлинности электронной подписи в электронном документе и/или предоставить информацию о статусе сертификата ключа проверки электронной подписи в порядке, предусмотренном в п.5.3 настоящего Регламента.

4.4.6. Наделять Доверенных лиц полномочиями по установлению личности Заявителя, проверке и приему документов, по вручению СКПЭП от имени УЦ.

4.4.7. Отказать в изготовлении СКПЭП Заявителю в случае, если использованный Заявителем формат запроса на изготовление СКПЭП не поддерживается УЦ или доверенной информационной системой.

4.4.8. Требовать от Субъекта, присоединившегося к Регламенту, безусловного выполнения всех его положений.

4.4.9. Изменять требования к структуре и составу полей сертификата по требованию заявителя и информационной системы, где будет использоваться СКПЭП.

4.4.10. Вносить сведения в сертификат на английском языке по требованию заявителя и информационной системы, где будет использоваться СКПЭП.

4.4.11. Изменять перечень пакета документов и сведений, предусмотренных в Приложении №1 настоящего Регламента.

4.5. Владелец сертификата имеет право:

4.5.1. Получить СКПЭП в форме электронного документа и/или на бумажном носителе.

4.5.2. Применять сертификат УЦ для проверки электронной подписи УЦ в СКПЭП и СОС, созданных УЦ.

4.5.3. Обратиться в УЦ для подачи заявления на прекращение действия СКПЭП в течение срока действия, соответствующего ключу электронной подписи.

4.5.4. В порядке, предусмотренном настоящим Регламентом, обратиться в УЦ для проверки подлинности электронной подписи электронного документа и/или предоставления информации о статусе СКПЭП в порядке, предусмотренном в п.5.3 настоящего Регламента.

5. Порядок и сроки выполнения процедур, необходимых для предоставления услуг Удостоверяющим центром, в том числе требования к документам, предоставляемым в Удостоверяющий центр в рамках предоставления услуг

5.1. Процедура создания ключей электронной подписи и ключей проверки электронной подписи (совместно именуемые далее по тексту - ключи):

5.1.1. Создание ключей осуществляется либо Заявителем самостоятельно, либо сотрудником УЦ. Одновременно с изготовлением ключей производится формирование файла с запросом на СКПЭП согласно процедуре, описанной в разделе 5.2.3 Регламента.

Описание способов создания ключей:

а) Заявитель самостоятельно создаёт ключи на своём рабочем месте с использованием руководства пользователя доверенной информационной системы, предоставленной

Удостоверяющим центром, либо с использованием собственных средств электронной подписи.

b) В Удостоверяющем центре ключи создает Заявитель или сотрудник УЦ для Заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), на автоматизированном рабочем месте, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, размещенном в служебном помещении, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается только на ключевой носитель владельца ключа.

5.1.2. Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной неквалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи», создаются с использованием средства электронной подписи.

Факт создания ключа электронной подписи и соответствующего ему ключа проверки электронной подписи, содержащегося в СКПЭП, Удостоверяющим центром, или факт создания данных ключей Владельцем СКПЭП самостоятельно при помощи средств электронной подписи, выданных ему Удостоверяющим центром, подтверждается фактом ознакомления под роспись с информацией, указанной в СКПЭП, согласно требованиям п. 4.2.2 настоящего Регламента и является документом, подтверждающим владение ключом проверки, указанного в составе данной информации.

5.1.3. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, порядок информирования владельцев СКПЭП об осуществлении такой смены с указанием доверенного способа получения нового сертификата Удостоверяющего центра:

5.1.3.1. Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ.

5.1.3.2. Плановая смена ключей ЭП УЦ производится по следующим основаниям:

- истечение срока использования ключа ЭП;
- переход на использование новых стандартов ЭП и функции хеширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования электронной подписи.

5.1.3.3. Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

- УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП уполномоченного лица УЦ;
- УЦ осуществляет информирование Заявителей/Владельцев СКПЭП о проведении плановой смены ключей уполномоченного лица удостоверяющего центра (о вводе в действие нового сертификата издателя сертификатов) посредством публикации информации на официальном сайте Удостоверяющего центра по адресу: https://www.esphere.ru. Доверенным способом получения нового сертификата УЦ является его публикация на официальном сайте Удостоверяющего центра по адресу: https://www.esphere.ru, доступная для скачивания.

Старые ключи УЦ Удостоверяющий центр использует в течение их срока действия для формирования СОС, изданных УЦ в период действия старых ключей ЭП УЦ.

- Все Заявители/Владельцы СКПЭП должны установить на своих компьютерах/рабочих местах новый сертификат УЦ.

5.1.4. Порядок осуществления внеплановой смены ключей электронной подписи Удостоверяющего центра, в т.ч. в случаях нарушения их конфиденциальности:

5.1.4.1. Основания для внеплановой смены ключей УЦ:

- ключ электронной подписи УЦ закончил свой срок действия, а плановая смена

произведена не была;

- произошла компрометация ключа электронной подписи УЦ;
- есть подозрение, что ключ электронной подписи УЦ мог быть скомпрометирован;
- ключ электронной подписи УЦ не доступен (ключевой носитель поврежден, уничтожен и т.д.);
- в связи с необходимостью генерации новых ключей электронной подписи ЭП УЦ (например, в связи с введением новых Требований к форме или формату сертификата и т.д.);
- по решению, вступившему в законную силу (по решению суда, по решению владельца удостоверяющего центра и т.д.).

Актуальными угрозами нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра являются:

a) Угрозы, реализуемые по локальной сети:
   - осуществление доступа к файлам БД АС путем использования неправомерно полученных аутентификационных данных для подключения с помощью средств (служб) удаленного доступа, функционирующих на сервере базы данных автоматизированной системы.

b) Угрозы, связанные с непосредственным доступом:
   - хищение сетевого оборудования, линий связи.

c) Непреднамеренно реализуемые угрозы:
   - нарушение функционирования локальной сети, влекущее недоступность сервера базы данных автоматизированной системы, вызванное сбоем в функционировании сетевого оборудования, повреждением линий связи или отказом (сбоем) сетевых служб.

5.1.4.2. Процедура внеплановой смены ключей УЦ выполняется в порядке, определённом процедурой плановой смены ключей УЦ.

5.1.4.3. В случае компрометации ключа ЭП УЦ сертификат УЦ досрочно прекращает свой срок действия, Заявители/владельцы СКПЭП извещаются УЦ об указанном факте путем публикации информации о компрометации на сайте УЦ по адресу: https://www.esphere.ru. Все СКПЭП, подписанные с использованием скомпрометированного ключа УЦ, досрочно прекращают действие, с занесением соответствующих сведений об этих сертификатах в СОС.

Доверенным способом получения нового сертификата УЦ является его публикация на официальном сайте Удостоверяющего центра по адресу: https://www.esphere.ru, доступная для скачивания.

Все Заявители/Владельцы СКПЭП должны установить на своих компьютерах/рабочих местах новый сертификат УЦ.

5.1.5. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца СКПЭП:.

5.1.5.1. Смена ключа ЭП владельца СКПЭП осуществляется в случаях:

- истечения срока действия СКПЭП;
- на основании заявления владельца СКПЭП о досрочном прекращении его действия (согласно Приложения № 2 к Регламенту), подаваемого в форме документа на бумажном носителе или в форме электронного документа в порядке, описанном в п.5.4 Регламента;
- если не подтверждено, что владелец сертификата ключа проверки ЭП владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;
- если установлено, что содержащийся в таком СКПЭП ключ проверки ЭП уже содержится в ином ранее созданном сертификате ключа проверки ЭП;
- если вступило в силу решение суда, которым, в частности, установлено, что СКПЭП содержит недостоверную информацию;
- иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в

соответствии с ними нормативными правовыми актами или соглашением между УЦ и Заявителем и/или Клиентом УЦ.

5.1.5.2. При смене ключа ЭП Заявитель подает заявление на изготовление СКПЭП в соответствии с требованиями раздела 5.2. настоящего Регламента.

5.2. Процедура создания и выдачи СКПЭП для Владельцев:

5.2.1. Порядок подачи заявления на создание и выдачу СКПЭП и требования к нему.

Создание и выдача СКПЭП осуществляется на основании заявления на изготовление такого сертификата, оформленного Заявителем/Клиентом УЦ и/или Владельцем СКПЭП по форме предоставленной Удостоверяющим центром Заявителю/Клиенту УЦ в доверенной информационной системе или посредством направления электронной почтой, в том числе по форме согласно соглашению/договору[1], с предоставлением документов, указанных в Приложении № 1 к Регламенту и отдельно запрашиваемых УЦ документов (при необходимости)[2](далее по тексту – пакет документов).

Заявление на изготовление СКПЭП (далее по тексту – заявление) предоставляется в УЦ либо в форме документа на бумажном носителе, либо в форме электронного документа. Подписание заявления в форме документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета, а в форме электронного документа – способом, указанным в п.1 ч.1 ст. 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», ()или иным видом электронной подписи, который прямо предусмотрен соглашением/договором между Субъектами.

Сотрудник УЦ/ доверенное лицо УЦ в момент принятия заявления на изготовление СКПЭП к рассмотрению выполняет процедуру идентификации лица, обратившегося в УЦ, путем установления личности обратившегося согласно п.5.2.2. Регламента.

После положительного результата процедуры идентификации обратившегося лица сотрудник/доверенное лицо УЦ принимает к рассмотрению пакет документов, и осуществляет следующие действия:

1) проверяет данные в заявлении на изготовление СКПЭП на соответствие данным, содержащимся в иных представленных Заявителем документах, на полноту, достаточность и достоверность внесенных сведений (информации) и представленных документов, в том числе на соответствие настоящему Регламенту;
2) устанавливает:
   - факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно представляет;
   - факт соответствия сведений, указанных в заявлении, представленным документам;
   - факт отсутствия признаков подделки представленных документов.

В случае, если полученные из государственных информационных ресурсов сведения (при использовании такой проверки при создании СКПЭП) подтверждают достоверность информации, представленной Заявителем для включения в СКПЭП, и УЦ (его Доверенным лицом) установлена личность Заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени Заявителя – юридического лица, на обращение за получением СКПЭП, УЦ принимает решение о принятии пакета документов и осуществляет процедуру создания и выдачи СКПЭП (п.5.2.3 Регламента). В противном случае, УЦ отказывает Заявителю в принятии пакета документов и в выдаче СКПЭП.

При отклонении заявления на изготовление СКПЭП сотрудник/доверенное лицо УЦ уведомляет об этом обратившееся лицо с указанием причины отклонения пакета документов.

---

[1] Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Заявителя УЦ/Клиента УЦ.

[2] УЦ оставляет за собой право запросить у Субъекта, дополнительные документы: в случае, предусмотренном законодательством, или при установлении информационными системами, дополнительных требований к СКПЭП пользователей для работы в соответствующих информационных системах в целях обеспечения информационной безопасности.

Если для подтверждения каких-либо сведений, вносимых в СКПЭП, действующим законодательством РФ установлена определенная форма документа, Заявитель УЦ представляет документ соответствующей формы.

При принятии заявления на изготовление СКПЭП сотрудник/доверенное лицо УЦ проставляет отметку о принятии на заявлении и/или иным образом подтверждает факт принятия такого пакета документов.

Субъект, присоединившийся к Регламенту, обязан предоставлять в Удостоверяющий центр только достоверную информацию. В случае если после создания СКПЭП выяснится факт предоставления поддельных копий документов, Удостоверяющий центр вправе в одностороннем порядке прекратить действие такого сертификата, а Субъект несет материальную ответственность в размере стоимости оказанных услуг УЦ и другие неблагоприятные последствия, предусмотренные законодательством РФ.

На основе принятого пакета документов сотрудник УЦ выполняет действия по занесению регистрационной информации в базу данных УЦ, а также действия по формированию ключей электронной подписи, изготовлению и выдаче СКПЭП (п.5.2.3 Регламента)

Если владельцем СКПЭП является юридическое лицо, то наряду с наименованием такого юридического лица в СКПЭП может вноситься информация о представителе юридического лица (физическом лице), указанном в заявлении на изготовлении СКПЭП.

Получение ключей электронной подписи, СКПЭП, информации, содержащейся в нем может быть осуществлено только Заявителем УЦ, владельцем СКПЭП.

В случае внесения в СКПЭП персональных данных физического лица, Заявитель УЦ и/или владелец СКПЭП предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия может быть включен в заявление на изготовление СКПЭП и подписывается Владельцем СКПЭП.

5.2.2. Порядок установления личности заявителя.

Идентификация Заявителя устанавливается одним из следующих способов:

a) При личном присутствии Заявителя в Удостоверяющем центре или у Доверенного лица Удостоверяющего центра.

Сотрудник УЦ/Доверенное лицо УЦ выполняет процедуру идентификации Заявителя УЦ путем установления его личности по документам, удостоверяющим личность. Для его идентификации требуется только оригинал соответствующего документа, удостоверяющего личность.

Порядок идентификации Заявителя следующий:

- идентификация гражданина Российской Федерации осуществляется по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;

- идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

- идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

b) Без личного присутствия Заявителя:

- с использованием его УКЭП при наличии КСКПЭП, действующего на момент подачи заявления, который принадлежит лицу, личность которого устанавливается.

- путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации,

содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 08.11.2019 г. № 1427 »О проведении эксперимента по совершенствованию применения технологии электронной подписи» (;

- путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27.07.2006 г. « 149-ФЗ «Об информации, информационных технологиях и о защите информации» .

- с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации, и при условии организации взаимодействия удостоверяющего центра с единой системой идентификации и аутентификации, гражданами (физическими лицами) и организациями с применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации:

- с использованием усиленной неквалифицированной электронной подписи, сертификат ключа проверки которой создан и используется в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, в установленном Правительством Российской Федерации порядке, предусматривающем в том числе порядок проверки такой электронной подписи, и при условии организации взаимодействия физического лица с указанной инфраструктурой с применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

- иным способом, разрешенным Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

5.2.3. Порядок и сроки создания и выдачи СКПЭП.

При принятии заявления на изготовление СКПЭП и пакета документов согласно процедур, описанных в п.5.2.1 и п.5.2.2 Регламента, создание ключей ЭП и СКПЭП осуществляется в течение не более 5 (пяти) рабочих дней, если другой срок не предусмотрен в соглашении/договоре между Субъектами.

а) Процедура создания ключей в УЦ (точке выдачи), имеющей соответствующую лицензию на право осуществления деятельности включает в себя:

- внесение регистрационной информации в отношении будущего Владельца СКПЭП в базу данных УЦ;
- создание ключей, устанавливаемых на носитель, допустимого эксплуатационной документацией к СКЗИ УЦ;
- формирование запроса на создание СКПЭП;
- непосредственно изготовление СКПЭП;
- установка СКПЭП в соответствующий контейнер;
- ознакомление Заявителя с информацией, содержащейся в СКПЭП, собственноручно или способом, определенным в доверенной информационной системе;
- внесение данных об изготовленных СКПЭП и ключевых носителях в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- передача Владельцу СКПЭП носителя (при использовании носителя Владельца СКПЭП) с ключевой парой под роспись в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, сотрудником/доверенным лицом УЦ.

б) Процедура создания ключей электронной подписи и запроса на СКПЭП Заявителем самостоятельно включает в себя:

- получение уведомления от УЦ о необходимости создания ключей электронной

подписи и запроса на СКПЭП на своем персональном компьютере с использованием средств СКЗИ;

- в случаях, предусмотренных условиями договора, Субъекту УЦ может быть предоставлен доступ к доверенной информационной системе, с возможностью создания запроса на изготовление СКПЭП[3];
- предоставление запроса на сертификат в УЦ для изготовления СКПЭП;
- проверка сведений в запросе;
- изготовление СКПЭП непосредственно УЦ;
- ознакомление Заявителя с информацией, содержащейся в СКПЭП, собственноручно или способом, определенным в доверенной информационной системе;
- получение Владельцем СКПЭП СКПЭП соответствующего его ключу электронной подписи;
- установка СКПЭП его Владельцем в соответствующий ключевой контейнер.

При использовании доверенной информационной системы для создания и выдачи СКПЭП, ознакомление с информацией, содержащейся в СКПЭП, осуществляется в электронном виде, в качестве подтверждения такого ознакомления используется простая электронная подпись (ПЭП), НЭП или усиленная квалифицированная электронная подпись. При таком ознакомлении информация, содержащаяся в СКПЭП, отдельно на бумажном носителе не предоставляется.

Субъекты УЦ соглашаются использовать ПЭП в порядке и на условиях настоящего Регламента и/или отдельно заключаемых соглашений/договоров. В соответствии с соглашением об использовании ПЭП в доверенной системе УЦ, ключом ПЭП является пароль входа в систему УЦ. В сочетании установленных системой фактов успешных идентификации и аутентификации субъекта с подтверждением им уникального случайно генерируемого кода аутентификации полученного автоматически и отправленного Удостоверяющим центром в форме SMS-сообщения на зарегистрированный номер подвижной (мобильной) связи Владельца СКПЭП, в период его авторизованной сессии после установки в соответствующем поле доверенной информационной системы признака ознакомления с СКПЭП, позволяет Удостоверяющему центру считать данную информацию подписанной ПЭП и доверять этой информации.

Владелец СКПЭП обязан хранить в тайне ключ ПЭП, принимать все возможные меры, предотвращающие нарушение его конфиденциальности. В случае нарушения конфиденциальности ключа ПЭП Владелец СКПЭП обязан незамедлительно уведомить об этом Удостоверяющий центр.

Информация в электронной форме, подписанная ПЭП или НЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Владельца СКПЭП.

5.3. Порядок предоставления информации о статусе СКПЭП и/или проверки подлинности электронной подписи в электронном документе:

Предоставление информации о статусе СКПЭП и/или проверка подлинности электронной подписи в электронном документе осуществляется УЦ на возмездной основе. Особенности проведения работ, конкретный перечень требуемых исходных данных, сроки проведения таких работ, их стоимость и иные условия определяются сторонами в рамках отдельного договора (соглашения).

После заключения договора/соглашения УЦ приступает к выполнению работ соответственно по заявлению на предоставление информации о статусе СКПЭП, созданного УЦ (Приложение № 3 к настоящему Регламенту), или по заявлению на проверку подлинности электронной подписи электронного документа (Приложение № 4 к настоящему Регламенту).

Оформленное заявление предоставляется в УЦ Заявителем УЦ в форме документа на бумажном носителе или в форме электронного документа. Подписание заявления в форме

[3] Особенности аутентификации владельца СКПЭП в данной доверенной информационной системы и работы в ней регулируются руководствами пользователя и/или отдельно заключаемыми договорами/соглашениями.

документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета, а в форме электронного документа - производится усиленной квалифицированной электронной подписью или иным видом электронной подписи, который прямо предусмотрен соглашением/договором между Субъектами.

Обязательным приложением к заявлению на проверку подлинности электронной подписи в электронном документе является носитель, содержащий файл СКПЭП, подвергающийся процедуре проверки.

Сотрудник/доверенное лицо УЦ проверяет полноту и достаточность внесенных сведений/предоставленных приложений и при достаточности - проставляет на заявлении обратившегося лица отметку о получении и/или принятии такого заявления, при недостаточности – сообщает об этом Заявителю УЦ с указанием причин.

По результатам проведения работ, УЦ оформляет в произвольной форме документ (справку, заключение и т.п.), содержащий соответственно информацию о статусе СКПЭП или о проверки подлинности электронной подписи электронного документа, заверенный подписью УЦ, в двух экземплярах, один из которых предоставляется Заявителю УЦ.

5.4. Процедуры, осуществляемые при прекращении действия или аннулирования СКПЭП:

УЦ осуществляет отзыв СКПЭП на основании заявления по форме Приложения № 2 к настоящему Регламенту, или форме документа, полученного в доверенной информационной системе, полученного в форме документа на бумажном носителе, либо в форме электронного документа. Подписание заявления в форме документа на бумажном носителе производится собственноручно (без применения факсимиле) чернилами (пастой) синего или черного цвета, а в форме электронного документа - производится усиленной квалифицированной электронной подписью или иным видом электронной подписи, который прямо предусмотрен соглашением/договором между Субъектами или Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

Сотрудник УЦ осуществляет идентификацию обратившегося лица и проверку наличия у него соответствующих полномочий, проверяет полноту и достаточность внесенных в заявление сведений.

В случае положительного результата проставляет отметку о принятии заявления. В случае отказа в прекращении действия СКПЭП УЦ уведомляет об этом Заявителя УЦ с указанием причин отказа.

СКПЭП прекращает свое действие в случаях, указанных в п. 4.4.4. настоящего Регламента, а также в следующих случаях, установленных статьей 14 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи»:

- в связи с истечением установленного срока его действия;
- на основании заявления Владельца СКПЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности УЦ без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом №63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и заявителем, а также настоящим Регламентом.

УЦ аннулирует СКПЭП, если:

- не подтверждено, что владелец СКПЭП владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в СКПЭП ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате;
- вступило в силу решение суда, которым установлено, что СКПЭП содержит недостоверную информацию.

До внесения в реестр сертификатов информации об аннулировании СКПЭП Удостоверяющий центр обязан уведомить Владельца СКПЭП об аннулировании его СКПЭП путем направления соответствующего документа на бумажном носителе или в форме электронного документа.

5.5. Порядок ведения реестра сертификатов:

Реестр сертификатов ключей проверки ЭП ведётся УЦ в электронной форме.

Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Хранение информации, содержащейся в реестре сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

Удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

Формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему. Для предотвращения утраты сведений о сертификатах, содержащихся в реестре, формируется его резервная копия. Удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов.

Информация о прекращении действия или аннулировании СКПЭП вносится в реестр сертификатов. Действие СКПЭП прекращается/аннулируется с момента публикации СОС, в который внесён этот СКПЭП. Срок внесения в СОС сведений о прекращении действия или аннулировании сертификата указан в п. 4.1.11. Регламента.

5.5.1. Порядок технического обслуживания реестра сертификатов.

Плановые технические работы по обслуживанию реестра сертификатов проводятся Удостоверяющим центром в выходные дни либо в ночное время (с учетом часовых поясов на территории Российской Федерации) с целью минимизации и возможности исключения перерывов в работе при использовании СКПЭП их Владельцами и в доступе к реестру сертификатов Удостоверяющего центра.

Внеплановые технические работы проводятся при появлении такой необходимости в оперативном режиме.

Максимальные сроки проведения технического обслуживания реестра сертификатов составляют не более 12 часов. Время проведения технического обслуживания может быть увеличено при наличии объективных оснований и причин.

УЦ оповещает лиц, использующих реестр сертификатов, о проведении планового или внепланового технического обслуживания реестра сертификатов путем публикации информации на официальном сайте УЦ.

6. Порядок исполнения обязанностей Удостоверяющего центра

6.1. Информирование Субъектов УЦ об условиях и о порядке использования средств электронной подписи, о рисках, связанных с их использованием и о мерах, необходимых для обеспечения безопасности ключей электронной подписи и процедур проверки электронных подписей осуществляется посредством вручения руководства по обеспечению безопасности использования сертификата электронной подписи и средств электронной подписи, содержимое которого определяет обязанность владельца СКПЭП, в порядке, описанном в разделе 5.2.3 Регламента, в том числе по обеспечению режима конфиденциальности информации.

6.2. Удостоверяющий центр по обращению заявителя выдает средства электронной подписи, отвечающие требованиям:

- средства ЭП позволяют установить факт изменения подписанного электронного документа после момента его подписания;
- средства ЭП обеспечивают практическую невозможность вычисления ключа

электронной подписи из электронной подписи или из ключа ее проверки;

- средства ЭП позволяют создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

При создании электронной подписи средства электронной подписи должны (не относится к средствам ЭП, используемым для автоматического создания ЭП):

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;
- создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
- однозначно показывать, что электронная подпись создана.

При проверке электронной подписи средства электронной подписи должны (не относится к средствам ЭП, используемым для автоматической проверки ЭП):

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью;
- показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;
- указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы

Средства ЭП, предназначенные для создания электронных подписей электронных документов, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

Средство электронной подписи должно противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой средством электронной подписи информации или с целью создания условий для этого.

Средство ЭП должно проводить аутентификацию субъектов доступа (лиц, процессов) к этому средству, при этом:

- при осуществлении доступа к средству электронной подписи аутентификация субъекта доступа должна проводиться до начала выполнения первого функционального модуля средства электронной подписи;
- механизмы аутентификации должны блокировать доступ этих субъектов к функциям средства ЭП при отрицательном результате аутентификации.

Средство ЭП должно проводить аутентификацию лиц, осуществляющих локальный доступ к средству электронной подписи.

Средства электронной подписи Удостоверяющего центра и передаваемые им средства электронной подписи Заявителям/Владельцам СКПЭП удовлетворяют требованиям Федерального закона от 23 06.04.2011 № 63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. №796.

6.3. Обеспечение актуальности информации в реестре сертификатов и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий.

УЦ обеспечивает актуальность информации, содержащейся в реестре сертификатов, защиту информации от неправомерного доступа, уничтожения, модификации, блокирования и иных

неправомерных действий. Актуальность обеспечивается путем своевременного внесения записи о выпуске, прекращении действия или аннулировании СКПЭП в реестр сертификатов. Режим защиты является общим требованием в отношении всей сферы применения электронной подписи, он обеспечивается посредством применения специальных шифровальных средств, способствующих защите информации от несанкционированного доступа.

6.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронной подписи.

6.5.1. Требования к обеспечению конфиденциальности.

Необходимо немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

Запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ (в т.ч. средства усиленной электронной подписи), после ввода ключевой информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- оставлять без присмотра ключевые носители (на столе, подключенным к ПЭВМ и пр.);
- разглашать пароль (пин-код) ключевого носителя и допускать использование принадлежащих им ключей электронной подписи без их согласия;
- применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

Ключи ЭП на ключевом носителе защищаются паролем (пин-кодом).

6.5.2. Условия временного хранения ключей электронной подписи.

- при хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец несет персональную ответственность за хранение личных ключевых носителей;
- в случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

6.5.3. Сроки уничтожения ключей электронной подписи.

Ключи на ключевых носителях в том числе срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Срок уничтожения ключей электронной подписи Владелец устанавливает самостоятельно.

7. Сроки действия ключевых документов

Срок действия, изготовленного УЦ, СКПЭП указан в полях «notBefore» и «not After» поля «Validity» сертификата.

Начало периода действия ключа электронной подписи исчисляется с даты и времени начала действия СКПЭП.

Время начала периода действия СКПЭП и его окончания заносится Удостоверяющим центром в поля «notBefore» и «not After» поля «Validity» СКПЭП соответственно.

Срок действия СКПЭП Удостоверяющего центра составляет не более 15 лет.

Максимальный срок действия ключа электронной подписи Владельца СКПЭП устанавливается эксплуатационной документацией средства электронной подписи (системы криптографической защиты информации), с использованием которого такой ключ создается.

Начало периода действия ключа электронной подписи Владельца СКПЭП исчисляется с момента начала действия СКПЭП, соответствующего данному ключу.

Срок действия СКПЭП, создаваемого Удостоверяющим центром для Владельца, равен сроку действия ключа электронной подписи, соответствующего данному СКПЭП.

8. Конфиденциальность информации

Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего СКПЭП.

9. Ответственность Субъектов

9.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту Субъекты несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного стороне неисполнением или ненадлежащим исполнением обязательств другой стороной. Ни один из Субъектов не отвечает за неполученные доходы (упущенную выгоду), которые бы получены другим Субъектом.

9.2. Субъекты не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой стороной настоящего Регламента своих обязательств.

9.3. Удостоверяющий центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в пакете документов, необходимых для создания СКПЭП.

9.4. Удостоверяющий центр несет ответственность за убытки при использовании владельцем СКПЭП ключа проверки электронной подписи и соответствующего СКПЭП только в случае, если данные убытки возникли при компрометации ключа проверки электронной подписи Удостоверяющего центра.

9.5. Ответственность сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

10. Условия обеспечения бесперебойности и отказоустойчивости удостоверяющего центра

10.1. Инженерно-технические меры защиты информации.

Программно-аппаратные средства и системы жизнеобеспечения УЦ обеспечивают возможность его надежного и непрерывного функционирования при отключении централизованного энергоснабжения.

10.2. Физический доступ в помещения.

Доступ в помещения УЦ регулируется Инструкцией по организации пропускного режима в ООО «КОРУС Консалтинг СНГ» и матрицей доступа. Рабочее помещение УЦ оборудовано запирающейся на замок дверью и опечатывается, в нерабочее время помещение сдается под охрану.

10.3. Охрана здания и помещений.

Административное здание, в котором размещен УЦ, оборудовано системой видеонаблюдения, охранной, пожарной сигнализацией и находится под защитой вневедомственной охраны.

10.4. Электроснабжение.

Технические средства УЦ в ежедневном режиме подключены к общегородской сети электроснабжения. Электрические сети и электрооборудование, используемые в УЦ, отвечают правилам устройства электроустановок, правилам технической эксплуатации электроустановок потребителей, правилам техники безопасности при эксплуатации электроустановок потребителей.

Технические средства УЦ подключены к источнику бесперебойного питания, обеспечивающего их работу в течение 30 минут после прекращения основного электроснабжения.

10.5. Система кондиционирования воздуха.

Помещение УЦ оборудовано системой кондиционирования воздуха. Система обеспечивает постоянное поддержание температурно-влажностного режима.

10.6. Противопожарная защита.

Помещение УЦ оборудовано системой пожарной сигнализации и автоматического пожаротушения. Пожарная безопасность помещений УЦ обеспечивается в соответствии с нормами и требованиями СНиП.

10.7. Программно-аппаратные меры защиты информации.

10.7.1. Организация доступа к техническим средствам Удостоверяющего центра.

Доступ к техническим средствам УЦ, размещенным в рабочем помещении, регулируется системой доступа в помещения. Контроль целостности технических средств УЦ обеспечивается опечатыванием дверей препятствующем неконтролируемому доступу.

10.7.2. Организация доступа к программным средствам УЦ.

Доступ к защищаемым информационным ресурсам УЦ ограничен использованием сертифицированных средств защиты информации.

УЦ имеет физическую связь с локально вычислительной сетью ООО «КОРУС Консалтинг СНГ» и с информационными сетями общего доступа через межсетевой экран, сертифицированный по требованиям ФСБ.

10.7.3. Резервное копирование.

Программно-аппаратные средства УЦ обеспечивают ежедневное резервное копирование баз данных УЦ.

10.7.4. Состояние безопасности УЦ.

Принятые меры физической безопасности обеспечивают:

- своевременное пресечение попыток несанкционированного проникновения в здание (помещения) УЦ;
- возможность задержания нарушителей силами охраны;
- сохранность материальных ценностей и документов;
- предупреждение происшествий и своевременную ликвидацию их последствий.

11. Список приложений

11.1. Приложение № 1. Перечень документов, представляемых Заявителем УЦ для изготовления

11.2. Приложение № 2. Форма заявления на прекращение действия СКПЭП.

11.3. Приложение № 3. Форма заявления на предоставление информации о статусе СКПЭП, созданного Удостоверяющим центром ООО «КОРУС Консалтинг СНГ».

11.4. Приложение № 4. Форма заявления на проверку подлинности электронной подписи в электронном документе.

Приложение №1
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «27» декабря 2023г.

Перечень документов, либо их надлежащим образом заверенные копии и сведения, представляемые заявителем для изготовления и включения в сертификат ключа проверки электронной подписи[4]

Для юридических лиц:

1. Заявление на изготовление сертификата ключа проверки электронной подписи.
2. Документ, подтверждающий правомочия заявителя обращаться от имени юридического лица за получением сертификата.
3. Основной документ, удостоверяющий личность владельца СКПЭП, в соответствии с действующим законодательством Российской Федерации.
4. Номер страхового свидетельства государственного пенсионного страхования заявителя – СНИЛС владельца СКПЭП.
5. Идентификационный номер налогоплательщика – ИНН Владельца СКПЭП (при наличии)
6. Идентификационный номер налогоплательщика юридического лица – ИНН ЮЛ

Для иностранных организаций:

1. Заявление на изготовление сертификата ключа проверки электронной подписи.
2. Основной документ, удостоверяющий личность владельца СКПЭП, в соответствии с действующим законодательством Российской Федерации.
3. Номер страхового свидетельства государственного пенсионного страхования заявителя – СНИЛС владельца СКПЭП.

Для индивидуальных предпринимателей:

1. Заявление на изготовление сертификата ключа проверки электронной подписи.
2. Основной документ, удостоверяющий личность владельца СКПЭП.
3. Номер страхового свидетельства государственного пенсионного страхования заявителя - СНИЛС владельца СКПЭП.
4. Основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя.
5. Идентификационный номер налогоплательщика заявителя - индивидуального предпринимателя.

Для физических лиц:

1. Заявление на изготовление сертификата ключа проверки электронной подписи.
2. Основной документ, удостоверяющий личность заявителя.
3. Номер страхового свидетельства государственного пенсионного страхования заявителя - СНИЛС владельца СКПЭП.
4. Идентификационный номер налогоплательщика заявителя – физического лица (при наличии).

В целях настоящего документа под надлежащим образом удостоверенными копиями документов понимаются копии:

- для юридических лиц – заверенные нотариусом или лицом, действующим от имени юридического лица без доверенности, либо уполномоченным сотрудником Заявителя (Клиента), с предоставлением копии документа, подтверждающего полномочия.

Многостраничные копии либо должны быть прошиты и заверены на листе сшивки, либо на каждой странице такой копии должна иметься отдельная заверительная надпись. Образец заверительной надписи:

Копия верна
Подпись / Должность/ ФИО
Дата
М.П. (при ее наличии)

- для индивидуальных предпринимателей и физических лиц - заверенные нотариусом.

В случае, если для подтверждения сведений, вносимых в сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Для установления личности владельца СКПЭП в Удостоверяющий центр представляется только оригинал основного документа, удостоверяющего его личность.

В случае представления заявителем оригиналов документов Удостоверяющий центр осуществляет их копирование, для хранения в Удостоверяющем центре. Делается копия основного документа, удостоверяющего личность доверенного лица.

[4] В соответствии с п.4.4.10 и п.4.4.11 перечень документов может быть изменен для любого типа Клиента. Удостоверяющий центр вправе запросить иные документы, подтверждающие сведения, содержащиеся в заявлении на изготовление СКПЭП и подлежащие внесению в сертификат электронной подписи.

ФОРМА

Приложение № 2
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «27» декабря 2023г.

Руководителю ООО «КОРУС Консалтинг СНГ»

Заявление на прекращение действия
сертификата ключа проверки электронной подписи

_____
полное наименование юридического лица, включая организационно-правовую форму либо статус и полные ФИО индивидуального предпринимателя либо полные ФИО физического лица

_____
должность и фамилия, имя, отчество руководителя юридического лица или уполномоченного сотрудника, либо серия и номер паспорта, дата выдачи и кем выдан – для ФЛ/ИП

действующий на основании _____
основание полномочий (устав, положение, доверенность №__ от___)

просит прекратить действие сертификата ключа проверки электронной подписи в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» и Регламентом Удостоверяющего центра ООО «КОРУС Консалтинг СНГ», содержащего следующие идентификационные данные:

Серийный (уникальный) номер сертификата			
ИНН (для ЮЛ/ИП/ФЛ)	ОГРН (для ЮЛ)		
Фамилия, имя и отчество владельца сертификата			
Должность владельца сертификата (для ЮЛ)			
Основание прекращения действия сертификата			

Лицо, подписывающее настоящее заявление, понимает и принимает на себя риск последствий, следующих за выбранным действием, направленным на прекращение действия сертификата ключа проверки электронной подписи.

_____	_____	_____
Должность руководителя или уполномоченного сотрудника ЮЛ/ИП	подпись	Ф.И.О.

МП (при наличии) «_____»_____20___г
.

Отметки уполномоченного лица Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:

Заявление принял и проверил на полноту и достоверность данных:

_____ _____ /_____/ «____» _____ 20__г.
(Должность) (Подпись) (ФИО) (Дата)

ФОРМА

Приложение №3
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «27» декабря 2023г.

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КОРУС Консалтинг СНГ»

_____
полное наименование юридического лица, включая организационно-правовую форму либо статус и полные ФИО индивидуального предпринимателя либо полные ФИО физического лица

_____
должность и фамилия, имя, отчество руководителя юридического лица или уполномоченного сотрудника (заполняется при необходимости)

действующий на основании _____
основание полномочий (устав, положение, доверенность №__ от___) (заполняется при необходимости)

просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КОРУС Консалтинг СНГ» и содержащего следующие идентификационные данные:

Серийный (уникальный) номер сертификата	
Наименование ЮЛ/ИП - владельца сертификата	
Фамилия, имя и отчество владельца сертификата	
ИНН и/или ОГРН ЮЛ/ИП (при наличии)	
Время (период времени), на момент наступления которого необходимо установить статус сертификата[5]	с ____часов ____мин МСК «_____»_____20___г. по _____часов ____мин МСК «_____»_____20___г.
Иная информация о владельце сертификата (контактный адрес электронной почты)	

_____ _____ _____
Должность руководителя или уполномоченного сотрудника ЮЛ/ИП | подпись | Ф.И.О.

МП (при наличии) «_____»_____20____г.

Отметки уполномоченного лица Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:

Заявление принял и проверил на полноту и достоверность данных:

_____ _____ /_____/ «____» _____ 20__г.
(Должность) (Подпись) (ФИО) (Дата)

[5] Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

ФОРМА

Приложение № 4
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «27» декабря 2023г.

Заявление на проверку подлинности электронной подписи электронного документа

_____
полное наименование юридического лица, включая организационно-правовую форму либо статус и полные ФИО индивидуального предпринимателя либо полные ФИО физического лица

_____
должность и фамилия, имя, отчество руководителя юридического лица или уполномоченного сотрудника (заполняется при необходимости)

действующий на основании _____
основание полномочий (устав, положение, доверенность №__ от___) (заполняется при необходимости)

просит проверить подлинность электронной подписи электронного документа в соответствии со следующими идентификационными данными:

1.Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе.

2. Файл, содержащий подписанные электронной подписью данные, на прилагаемом к заявлению носителе.

3. Время подписания электронной подписью электронного документа:

_____часов _____мин МСК «____»_____20___г.

Если момент подписания электронного документа не определен, то необходимо указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

_____часов _____мин МСК «____»_____20___г.

Должность руководителя или уполномоченного сотрудника ЮЛ/ИП	подпись	Ф.И.О.

МП (при наличии) «_____»_____20____г.

Отметки уполномоченного лица Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:			
Заявление принял и проверил на полноту и достоверность данных:			
_____ (Должность)	_____ (Подпись)	/_____/ (ФИО)	«____» _____ 20__г. (Дата)