

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


**Вершков С.В.
«03» февраля 2017 г.**



**Регламент
Удостоверяющего Центра
ООО «КОРУС Консалтинг СНГ»**

г. Санкт-Петербург
2017г.

1. Основные понятия

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

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 доверенным лицом Удостоверяющего центра изготовленного этим Удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Доверенное лицо Удостоверяющего центра – физическое лицо, наделенное полномочиями по проверке и приему документов, вручению квалифицированных 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 .

Квалифицированный сертификат ключа проверки электронной подписи (далее – КСКПЭП) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом «Об электронной подписи» 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Клиент Удостоверяющего центра – юридическое лицо, индивидуальный предприниматель или физическое лицо, обратившееся в Удостоверяющий центр для выпуска квалифицированного сертификата ключа проверки электронной подписи.

Ключевой носитель – аппаратное или программно-аппаратное устройство хранения ключей ЭП приобретаемое Клиентом и являющееся дополнительным 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.

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.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 09:00 по 18:00 (мск) каждого дня недели за исключением выходных и праздничных дней.

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.

2. Общие положения

2.1. Настоящий Регламент является руководящим документом Удостоверяющего центра ООО «КОРУС Консалтинг СНГ» (далее – Удостоверяющий центр Компании, УЦ) и представляет собой совокупность правил, которые обеспечивают безопасное функционирование Удостоверяющего центра, определяют условия предоставления и правила пользования услугами Удостоверяющего центра.

2.2. УЦ осуществляет целевые функции удостоверяющего центра в соответствии с требованиями действующей редакции Федерального закона № 63-ФЗ от 06.04.2012 «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами.

2.3. Удостоверяющий центр Компании осуществляет свою деятельность на территории Российской Федерации в качестве профессионального участника рынка услуг по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи (а равно, сертификаты ключей проверки электронной подписи).

Информация о наличии у Компании свидетельства об аккредитации Удостоверяющего центра в Минкомсвязи России размещена на сайте Компании в сети «Интернет» по адресу: www.esphere.ru/ в разделе «Лицензии и сертификаты».

Удостоверяющий центр осуществляет свою деятельность с использованием программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ».

2.4. 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.
Адрес Удостоверяющего центра: 194100, г.Санкт-Петербург, Б. Сампсониевский пр-кт, д.68, лит.Н, пом.1Н.

ИНН 7801392271

ОГРН 1057812752502

Контактный телефон: 8 (800) 100-8-812

Адрес электронной почты: help@esphere.ru

Сайт Компании: www.esphere.ru

2.5. Настоящий Регламент распространяется в форме электронного документа в сети интернет по адресу www.esphere.ru, в разделе Удостоверяющий центр.

2.6. Субъектами, на которых распространяется действие настоящего Регламента, являются все лица, которые в силу настоящего Регламента, договора или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Регламентом. Субъектами являются – заявитель, владелец КСКПЭП, заинтересованное лицо, Удостоверяющий центр.

2.7. Присоединение заинтересованного лица к настоящему Регламенту и оказание такому лицу 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 заявления на изготовление сертификата ключа проверки электронной подписи.

2.8. Изготовление квалифицированного сертификата ключа проверки электронной подписи осуществляется на возмездной основе на основании заявления на изготовление такого сертификата, оформленного заинтересованным лицом в соответствии с Приложениями № 1 или № 2 к настоящему Регламенту, с предоставлением пакета документов, перечисленных в п.5.1.1., Приложении № 3 к настоящему Регламенту.

Форма заявлений может изменяться по условиям договора.

Заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи предоставляется в Удостоверяющий центр либо в форме документа на бумажном носителе либо в форме электронного документа, подписанного электронной подписью уполномоченного лица.

Сотрудник/доверенное лицо Удостоверяющего центра проверяет полноту и достаточность внесенных сведений, проставляет на заявлении обратившегося лица отметку о получении и/или принятии заявления.

2.9. Внесение изменений в настоящий Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке путем опубликования новой редакции Регламента на официальном сайте Компании 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.

2.10. 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». В случае прекращения выполнения ООО «КОРУС Консалтинг СНГ» функций Удостоверяющего центра реестр выданных сертификатов передается головному удостоверяющему центру в соответствии с Федеральным законом «Об электронной подписи» 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами.

3. Перечень реализуемых Удостоверяющим центром функций

3.1. Создание и выдача сертификатов при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от его имени по обращению за получением данного сертификата с учетом требований, установленных пунктом 4 части 4 статьи 8 Федерального закона «Об электронной подписи».

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

3.3. Установление сроков действия сертификатов.

3.4. Аннулирование выданных Удостоверяющим центром Компании сертификатов.

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.

3.6. Ведение реестра выданных и аннулированных Удостоверяющим центром Компании сертификатов ключей проверки электронных подписей, в том числе включающего в себя информацию, содержащуюся в выданных этим Удостоверяющим центром сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращений или аннулирований.

3.7. Создание ключей электронных подписей и ключей проверки электронных подписей по обращению заявителей.

3.8. Проверка уникальности ключей проверки электронных подписей в реестре сертификатов.

3.9. Осуществление проверки электронных подписей по обращению участников электронного взаимодействия.

4. Права и обязанности Сторон

4.1. Удостоверяющий центр обязан:

4.1.1. Создать сертификат ключа проверки электронной подписи на основании оформленного заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи (Приложения № 1 и №2 к настоящему Регламенту), в соответствии с порядком, определенным в настоящем Регламенте. Выдать владельцу квалифицированный сертификат ключа проверки электронной подписи в форме электронного документа или на бумажном носителе.

4.1.2. Использовать для создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

4.1.3. Вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами.

4.1.4. Использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им сертификатов ключей проверки электронной подписи и других случаев, предусмотренных законодательством Российской Федерации.

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

4.1.6. Организовать свою работу по московскому времени. Удостоверяющий центр синхронизирует все свои программные и технические средства обеспечения деятельности.

4.1.7. Обеспечить уникальность идентификационных данных заявителя, владельцев сертификатов, заносяемых в сертификаты ключей проверки электронной подписи.

4.1.8. Обеспечить уникальность серийных номеров создаваемых квалифицированных сертификатов ключей проверки электронной подписи.

4.1.9. Обеспечить уникальность значений ключей проверки электронной подписи в созданных квалифицированных сертификатах ключей проверки электронной подписи.

4.1.10. Обеспечить сохранение в тайне созданного ключа электронной подписи.

4.1.11. Аннулировать сертификат ключа проверки электронной подписи на основании заявления на аннулирование сертификата (Приложение № 5 к настоящему Регламенту) в соответствии с порядком, определенным в настоящем Регламенте.

Заявитель Удостоверяющего центра заполняет такое заявление (Приложение № 5 к настоящему Регламенту) и направляет его в Удостоверяющий центр либо в форме документа на бумажном носителе, либо в форме электронного документа, подписанного электронной подписью уполномоченного лица.

Сотрудник/доверенное лицо Удостоверяющего центра осуществляет идентификацию обратившегося лица и наличие у него соответствующих полномочий, проверяет полноту и достаточность внесенных сведений, проставляет на заявлении обратившегося лица отметку о получении и/или принятии заявления.

4.1.12. Аннулировать сертификат ключа проверки электронной подписи на основании заявления заинтересованного лица (Заявителя Удостоверяющего центра, владельца сертификата, третьего лица) (Приложение № 5 к настоящему Регламенту) с приложением решения суда, вступившего в законную силу, подтверждающего, что сертификат ключа проверки электронной подписи содержит недостоверную информацию и подлежит аннулированию.

Порядок работы с таким заявлением предусмотрен в п.4.1.11 настоящего Регламента.

4.1.13. Официально уведомить о прекращении, аннулировании сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации актуальных реестров сертификатов, прекративших свое действие или аннулированных сертификатов на ресурсе по адресу: www.esphere.ru/assets/download/uc/korus_sng.crl и www.edinavigator.com/assets/download/uc/korus_sng.crl.

Период публикации актуальных реестров прекративших свое действие или аннулированных сертификатов – 12 часа.

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

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

4.1.16. В соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» направлять в единую систему идентификации и аутентификации сведения о лице, получившем сертификат ключа проверки электронной подписи, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

4.1.17. Выдавать владельцу сертификата ключа проверки электронной подписи руководство по обеспечению безопасности использования квалифицированной электронной подписи средств криптографической защиты информации (Приложение № 8 к настоящему Регламенту).

4.1.18. По желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию указанного лица в единой системе идентификации и аутентификации.

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

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

4.1.21. Строго соблюдать срок действия ключей электронной подписи Удостоверяющего центра, используемых для подписания создаваемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие.

4.1.22. Осуществлять иные действия по реализации прав, предоставленных Заявителю Удостоверяющего центра и/или владельцу сертификата 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, подтверждающие сведения, содержащиеся в заявлении на изготовление сертификата и подлежащие включению Удостоверяющим центром в квалифицированный сертификат ключа проверки электронной подписи. Перечни и порядок предоставления соответствующих документов приведены в Приложении № 3 к настоящему Регламенту.

4.3. Заявитель Удостоверяющего центра и/или владелец сертификата обязан:

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

4.3.2. Соблюдать требования руководства по обеспечению безопасности использования

квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение № 8 к настоящему Регламенту).

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

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

4.3.5. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие ограничения были установлены.

4.3.6. Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование сертификата ключа проверки электронной подписи (Приложение № 5 к настоящему Регламенту) в случае нарушения конфиденциальности или подозрения о нарушении конфиденциальности ключа электронной подписи.

4.3.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата в Удостоверяющий центр до момента официального уведомления Удостоверяющим центром об аннулировании сертификата, либо об отказе в аннулировании.

4.3.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован и действие которого прекращено.

4.4. Удостоверяющий центр имеет право:

4.4.1. Запрашивать у заявителя документы для подтверждения любой содержащейся в заявлении на создание и выдачу сертификата информации.

4.4.2. С использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем.

4.4.3. Запрашивать и получать из государственных информационных ресурсов:

- выписку из единого государственного реестра юридических лиц в отношении заявителя – юридического лица;
- выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя – индивидуального предпринимателя;
- выписку из Единого государственного реестра налогоплательщиков в отношении заявителя – иностранной организации.

4.4.4. Запросить у заявителя дополнительные, подтверждающие достоверность представленных им сведений документы в случае наличия противоречий между сведениями, представленными заявителем и сведениями, полученными Удостоверяющим центром в соответствии с частью 2.2 статьи 18 Федерального закона «Об электронной подписи».

4.4.5. Не принимать от заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации.

4.4.6. Отказать заявителю в выдаче сертификата в случае невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами.

4.4.7. Отказать владельцу сертификата в прекращении действия сертификата в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям.

4.4.8. Без заявления владельца сертификата прекратить действие сертификата в случае наличия у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности

ключа электронной подписи владельца сертификата, а также невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи, а также в случае появления у Удостоверяющего центра достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

4.4.9. Отказать в аннулировании сертификата ключа проверки электронной подписи в случае ненадлежащего оформления соответствующего заявления (Приложение № 5 к настоящему Регламенту).

4.4.10. 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.

4.4.11. По запросу Заявителя Удостоверяющего центра предоставить ему заверенные копии лицензий, сертификатов, свидетельств, выданных Удостоверяющему центру и указанных в настоящем Регламенте.

4.5. Заявитель Удостоверяющего центра и/или владелец сертификата имеет право:

4.5.1. Получить сертификат ключа проверки электронной подписи как в форме электронного документа, так и в форме документа на бумажном носителе.

4.5.2. По запросу получить выписку из реестров квалифицированных сертификатов, формирование которых осуществляется Удостоверяющим центром в порядке, предусмотренном законодательством Российской Федерации и настоящим Регламенте.

Запрос должен содержать сведения как о запрашиваемом, так и о заинтересованном лицах, а также указание на способ получения запрашиваемой выписки из реестра и контактные данные получателя.

Запрос о предоставлении информации из реестра квалифицированных сертификатов представляется в Удостоверяющий центр лично или направляется на бумажном носителе или в форме электронного документа, заверенного электронной подписью, по контактным адресам Удостоверяющего центра, указанным в настоящем Регламенте.

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

4.5.4. Применять информацию из реестра квалифицированных сертификатов, формирование которых осуществляется Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

4.5.5. Обратиться в Удостоверяющий центр для аннулирования квалифицированного сертификата ключа проверки электронной подписи в течение срока действия, соответствующего ключу электронной подписи.

4.5.6. В порядке, предусмотренном настоящим Регламентом, обратиться в Удостоверяющий центр для проверки подлинности электронной подписи в электронном документе и/или предоставления информации о статусе сертификата ключа проверки электронной подписи.

5. Порядок предоставления и пользования услугами Удостоверяющего центра

5.1. Порядок предоставления услуг Удостоверяющим центром:

5.1.1. Сотрудник/доверенное лицо Удостоверяющего центра в предварительно согласованный день перед принятием заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи (Приложение № 1 к настоящему Регламенту) к исполнению выполняет процедуру идентификации лица, обратившегося в Удостоверяющий центр, путем установления личности обратившегося.

Личность гражданина Российской Федерации устанавливается 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.

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учетом требований п. 2.8.

Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется 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.

Если для подтверждения каких-либо сведений, вносимых в сертификат, действующим законодательством установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Получение ключей электронной подписи и квалифицированного сертификата ключа проверки электронной подписи может быть осуществлено уполномоченным лицом Заявителя Удостоверяющего центра или владельца сертификата. В данном случае дополнительно представляется доверенность, выданная на имя представителя по форме согласно Приложению № 4 к настоящему Регламенту.

5.1.2. После положительной идентификации обратившегося лица сотрудник/доверенное лицо Удостоверяющего центра принимает к рассмотрению заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи по форме Приложения № 1 или № 2 к настоящему Регламенту с приложением документов, перечисленных в Приложении № 3 к настоящему Регламенту, проверяет полноту, достаточность и достоверность внесенных сведений (информации) и представленных документов, и принимает решение о формировании ключей электронной подписи и создании сертификата или об отказе в изготовлении.

5.1.3. В случае отказа в формировании ключей электронной подписи и в изготовлении квалифицированного сертификата сотрудник/доверенное лицо Удостоверяющего центра уведомляет об этом обратившееся лицо с указанием причины отклонения заявления.

5.1.4. При принятии положительного решения сотрудник/доверенное лицо Удостоверяющего центра проставляет на заявлении обратившегося лица отметку о получении и/или принятии заявления.

На основе предоставленных заявительных документов в день обращения сотрудник Удостоверяющего центра выполняет регистрационные действия по формированию ключей электронной подписи, по занесению регистрационной информации в реестр Удостоверяющего центра и изготовлению и выдаче квалифицированного сертификата ключа проверки электронной подписи.

5.1.5. Генерация ключей подписи осуществляется либо Заявителем самостоятельно (с использованием сертифицированных СКЗИ), либо сотрудником Удостоверяющего центра. Одновременно с изготовлением ключей подписи производится формирование файла с запросом на сертификат.

Сотрудник Удостоверяющего центра осуществляет генерацию ключей на автоматизированном рабочем месте, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, размещенном в аттестованном помещении, доступ в которое ограничен.

5.1.6. Изготовление сертификата осуществляется в порядке, предусмотренном в п.2.8 настоящего Регламента. Удостоверяющим центром в квалифицированный сертификат вносится информация на основании соответствующих документов, представленных обратившимся лицом.

5.1.7. Сотрудник/доверенное лицо Удостоверяющего центра ознакомливает под подпись владельца сертификата ключа проверки электронной подписи с руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение № 8 к настоящему Регламенту).

5.1.8. При получении сертификата заявитель подлежит обязательному ознакомлению под подпись с информацией, содержащейся в сертификате ключа проверки электронной подписи.

5.2. Порядок аннулирования сертификата ключа проверки электронной подписи:

5.2.1. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи по основаниям и в порядке, указанном в п. 4.1.11 – п. 4.1.13 настоящего Регламента. В случае отказа в аннулировании сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом Заявителя Удостоверяющего центра с указанием причин отказа.

5.2.2. Сертификат прекращает свое действие:

- по истечении срока его действия;
- на основании заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам;
- в иных случаях, установленных в Порядке в соответствии с законодательством Российской Федерации в области электронной подписи.

5.2.3. Удостоверяющий центр признает сертификат аннулированным, если:

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

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

5.3.1. Удостоверяющий центр по заявлению на предоставление информации о статусе квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром (Приложение № 6 к настоящему Регламенту) или на основании заявления на проверку подлинности электронной подписи в электронном документе (Приложение № 7 к настоящему Регламенту) предоставляет информацию о статусе сертификата ключа проверки электронной подписи и/или осуществляет проверку подлинности электронной подписи в электронном документе.

Оформленное заявление предоставляется в Удостоверяющий центр заинтересованным лицом в форме документа на бумажном носителе или в форме электронного документа, заверенного электронной подписью.

Сотрудник/доверенное лицо Удостоверяющего центра проверяет полноту и достаточность внесенных сведений и проставляет на заявлении обратившегося лица отметку о получении и/или принятии такого заявления.

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

Перечень исходных данных для проведения экспертных работ по проверки подлинности электронной подписи в электронном документе, сроки проведения таких работ, размер вознаграждения Удостоверяющего центра и иные условия определяются сторонами в рамках отдельного договора (соглашения).

По результатам проведения работ Удостоверяющий центр оформляет в произвольной форме документ (справку, заключение и т.п.), содержащий информацию о статусе сертификата ключа проверки электронной подписи и/или о проверки подлинности электронной подписи в электронном документе, заверенный подписью Удостоверяющего центра, в двух экземплярах, один из которых предоставляется Заявителю.

6. Сроки действия ключевых документов

Срок действия ключевых документов владельца сертификата и изготовленного сертификата указан в полях «notBefore» и «not After» поля «Validity» сертификата.

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

Время начала периода действия сертификата ключа проверки электронной подписи и его окончания заносится Удостоверяющим центром в поля «notBefore» и «not After» поля «Validity» квалифицированного сертификата соответственно.

7. Конфиденциальность информации

Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи.

8. Ответственность сторон

8.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного стороне неисполнением или ненадлежащим исполнением обязательств другой стороной. Ни одна из сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая сторона.

8.2. Стороны 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.

8.3. 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 соответствующих заявлениях, указанных в настоящем Регламенте.

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

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

9. Условия обеспечения безопасного формирования ключей электронной подписи и изготовления сертификатов ключей проверки электронной подписи

9.1. Инженерно-технические меры защиты информации.

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

9.2. Физический доступ в помещения.

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

9.3. Охрана здания и помещений.

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

9.4. Электроснабжение.

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

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

9.5. Система кондиционирования воздуха.

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

9.6. Противопожарная защита.

Помещение Удостоверяющего центра оборудовано системой пожарной сигнализации и автоматического пожаротушения. Пожарная безопасность помещений Удостоверяющего центра обеспечивается в соответствии с нормами и требованиями СНИП.

9.7. Программно-аппаратные меры защиты информации.

9.7.1. Организация доступа к техническим средствам Удостоверяющего центра.

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

9.7.2. Организация доступа к программным средствам Удостоверяющего центра.

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

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

9.7.3. Резервное копирование.

Программно-аппаратные средства Удостоверяющего центра обеспечивают ежедневное резервное копирование баз данных Удостоверяющего центра.

9.7.4. Состояние безопасности Удостоверяющего центра.

Принятые меры физической безопасности обеспечивают:

- своевременное пресечение попыток несанкционированного проникновения в здание (помещения) Удостоверяющего центра;
- возможность задержания нарушителей силами охраны;

- сохранность материальных ценностей и документов;
- предупреждение происшествий и своевременную ликвидацию их последствий.

10. Список приложений

10.1. Приложение №1. Форма Заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи Заявителя (Клиента) Удостоверяющего центра для заявителя - юридического лица, филиала юридического лица (в т.ч. для должностного лица).

10.2. Приложение №2. Форма Заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи Заявителя (Клиента) Удостоверяющего центра для заявителя - индивидуального предпринимателя, физического лица (гражданина РФ).

10.3. Приложение № 3. Перечень документов, представляемых заявителем для изготовления и включения в квалифицированный сертификат ключа проверки электронной подписи.

10.4. Приложение № 4. Форма доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи.

10.5. Приложение № 5. Форма заявления на аннулирование сертификата.

10.6. Приложение № 6. Форма заявления на предоставление информации о статусе квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КОРУС Консалтинг СНГ».

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

10.8. Приложение № 8. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

ФОРМА

Приложение №1
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.

Заявление
на изготовление квалифицированного сертификата ключа проверки электронной подписи
Заявителю (Клиенту) Удостоверяющего центра ООО «КОРУС Консалтинг СНГ» — юридическому лицу¹

_____ полное наименование юридического лица, включая организационно-правовую форму

_____ должность и фамилия, имя, отчество руководителя юридического лица или уполномоченного сотрудника

действующий на основании _____

_____ основание полномочий (устав, положение, доверенность № _____ от _____)

(далее — Заявитель УЦ) просит сформировать ключи электронной подписи и изготовить квалифицированный сертификат ключа проверки электронной подписи (далее — сертификат) согласно Федеральному закону №63-ФЗ от 06.04.2011 «Об электронной подписи» своему уполномоченному представителю, как владельцу сертификата ключа проверки электронной подписи, в соответствии со следующими идентификационными данными:

Краткое наименование ЮЛ	
ИНН ЮЛ	
ОГРН ЮЛ	
Юридический адрес ЮЛ	
Подразделение (заполняется при необходимости)	
Фамилия, имя, отчество владельца сертификата	
Должность владельца сертификата	
Номер страхового свидетельства государственного пенсионного страхования (СНИЛС) владельца сертификата	
Дата рождения владельца сертификата	
Гражданство владельца сертификата	
Пол владельца сертификата	
Место рождения владельца сертификата	
Серия и номер паспорта гражданина РФ (или иного основного документа, удостоверяющего личность)	
Дата выдачи паспорта гражданина РФ (или иного основного документа, удостоверяющего личность)	
Наименование органа выдавшего паспорт гражданина РФ (или иного основного документа, удостоверяющего личность)	
Код подразделения органа, выдавшего паспорт гражданина РФ	
Адрес электронной почты владельца сертификата	
Номер мобильного телефона владельца сертификата	
Информационная система, в которой предполагается использовать квалифицированный сертификат, иные ограничения его использования ²	

Я, _____ Владелец сертификата, зарегистрированный(-ая) по адресу:

_____ даю свое согласие ООО «КОРУС Консалтинг СНГ» (ОГРН 1057812752502, ИНН 7801392271), расположенному по адресу: 194100 г. Санкт-Петербург, Б. Сампсониевский пр-кт, д.68, литер Н помещение 1 «Н» (далее – Компания), в соответствии с Федеральным законом №152-ФЗ от 27.07.2006 «О персональных данных» на обработку моих персональных данных, указанных в настоящем Заявлении и в изготовленном сертификате. Настоящее согласие на обработку моих персональных данных дается мной в целях получения услуг и иных обязательств от Компании и/или других лиц, а также для возможности проверки авторства, подлинности и целостности моей электронной подписи в электронных документах лицами, в отношении с которыми допускается использование электронной подписи. В случае необходимости, также даю Компании право предоставлять мои персональные данные третьим лицам для выполнения Компанией принятых на себя обязательств, в том числе установленных законодательством Российской Федерации.

Данное согласие дается мной на весь период действия моего сертификата и до истечения сроков хранения информации или документов, содержащих вышеуказанную информацию, определяемых в соответствии с действующим законодательством Российской Федерации. Данное согласие может быть отозвано посредством направления Владелцем сертификата в Компанию письменного уведомления не менее чем за 30 (тридцать) календарных дней до момента отзыва данного согласия. После этого Компания вправе продолжать обработку персональных данных только в случаях, допускаемых действующим законодательством (п.2 ст.9, п.2-п.11ч.1 ст.6, ч.2 ст.10 и ч.2 ст.11 Закона о персональных данных).

Также я извещен(-а) о том, что неоформление (непредоставление в указанный срок) мной данного письменного согласия является основанием для Компании отказать/ограничить мне право использования и/или действие выданного сертификата. Настоящим, подтверждаю, что я ознакомлен(а) с опубликованным в сети Интернет по адресу: www.esphere.ru Регламентом Удостоверяющего центра Компании и обязуюсь его выполнять.

Владелец сертификата

_____ подпись

_____ Ф.И.О.

Настоящим, Заявитель УЦ и Владелец сертификата понимают и принимают на себя риск любых неблагоприятных последствий при указании в настоящем Заявлении неполной и/или недостоверной информации.

Владелец сертификата

_____ подпись

_____ Ф.И.О.

_____ Должность руководителя Заявителя или его представителя

_____ подпись

_____ Ф.И.О.

МШ

«___» _____ 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)

¹ Заполняется и представляется в одном экземпляре.

² Ограничения использования КСКП ЭП могут быть указаны в КСКП ЭП согласно подп.7 ч.2 ст.17 ФЗ от 06.04.2011 № 63-ФЗ. Между тем, возможные ограничения использования КСКП ЭП имеют организационно-уведомительный характер для контрагента и технически не позволяют заблокировать подписание.

ФОРМА

Приложение №2
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.

Заявление

на изготовление квалифицированного сертификата ключа проверки электронной подписи Заявителю (Клиенту)
Удостоверяющего центра ООО «КОРУС Консалтинг СНГ» - индивидуального предпринимателя, физического лица

полные ФИО владельца сертификата

серия и номер основного документа, удостоверяющего личность, кем и когда выдан

Статус ИП подтвержден записью из ЕГРИП о регистрации ИП за № _____ от «___» _____ 20__ г.

(далее – Заявитель УЦ) просит сформировать ключи электронной подписи и изготовить квалифицированный сертификат ключа проверки электронной подписи (далее – сертификат) согласно Федеральному закону №63-ФЗ от 06.04.2011 «Об электронной подписи» для себя как владельца такого сертификата в соответствии со следующими дополнительными идентификационными данными:

Фамилия, имя, отчество владельца сертификата	
Адрес регистрации	
ОГРНИП (для ИП)	
Номер страхового свидетельства государственного пенсионного страхования (СНИЛС)	
Идентификационный номер налогоплательщика (ИНН)	
Дата рождения владельца сертификата	
Гражданство владельца сертификата	
Пол владельца сертификата	
Место рождения владельца сертификата	
Серия и номер паспорта гражданина РФ (или иного основного документа, удостоверяющего личность) владельца сертификата	
Дата выдачи паспорта гражданина РФ (или иного основного документа, удостоверяющего личность)	
Наименование органа выдавшего паспорт гражданина РФ (или иного основного документа, удостоверяющего личность)	
Код подразделения органа, выдавшего паспорт гражданина РФ	
Адрес электронной почты владельца сертификата	
Номер мобильного телефона владельца сертификата	
Информационная система, в которой предполагается использовать квалифицированный сертификат, иные ограничения его использования ¹	

Я, Владелец сертификата, зарегистрированный(-ая) по адресу:

Консалтинг СНГ» (ОГРН 1057812752502, ИНН 7801392271), расположенному по адресу: 194100 г. Санкт-Петербург, Б. Сампсониевский пр-кт, д.68, литер Н помещение 1 «Н» (далее – Компания), в соответствии с Федеральным законом №152-ФЗ от 27.07.2006 «О персональных данных» на обработку моих персональных данных, указанных в настоящем Заявлении и в изготовленном сертификате. Настоящее согласие на обработку моих персональных данных дается мной в целях получения услуг и иных обязательств от Компании и/или других лиц, а также для возможности проверки авторства, подлинности и целостности моей электронной подписи в электронных документах лицами, в отношении с которыми допускается использование электронной подписи. В случае необходимости, также даю Компании право предоставлять мои персональные данные третьим лицам для выполнения Компанией принятых на себя обязательств, в том числе установленных законодательством Российской Федерации.

Данное согласие дается мной на весь период действия моего сертификата и до истечения сроков хранения информации или документов, содержащих вышеуказанную информацию, определяемых в соответствии с действующим законодательством Российской Федерации. Данное согласие может быть отозвано посредством направления Владелец сертификата в Компанию письменного уведомления не менее чем за 30 (тридцать) календарных дней до момента отзыва данного согласия. После этого Компания вправе продолжить обработку персональных данных только в случаях, допускаемых действующим законодательством (п.2 ст.9, п.2-п.11ч.1 ст.6, ч.2 ст.10 и ч.2 ст.11 Закона о персональных данных).

Также я извещен(-а) о том, что неоформление (непредоставление в указанный срок) мной данного письменного согласия является основанием для Компании отказать/ограничить мне право использования и/или действие выданного сертификата. Настоящим, подтверждаю, что я ознакомлен(а) с опубликованным в сети Интернет по адресу: www.esphere.ru Регламентом Удостоверяющего центра Компании и обязуюсь его выполнять.

Владелец сертификата

подпись

Ф.И.О.

Настоящим, Заявитель УЦ, он же Владелец сертификата, понимает и принимает на себя риск любых неблагоприятных последствий при указании в настоящем Заявлении неполной и/или недостоверной информации.

Тип Заявителя/Владельца сертификата
МПП (при наличии)

подпись

Ф.И.О.

«___» _____ 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)

¹ Ограничения использования КСКП ЭП могут быть указаны в КСКП ЭП согласно подп.7 ч.2 ст.17 ФЗ от 06.04.2011 № 63-ФЗ. Между тем, возможные ограничения использования КСКП ЭП имеют организационно-уведомительный характер для контрагента и технически не позволяют заблокировать подписание.

Приложение №3
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.

Перечень документов, представляемых заявителем для изготовления и включения в квалифицированный сертификат ключа проверки электронной подписи

Для юридических лиц		Для индивидуальных предпринимателей / физических лиц	
Владелец подписи - РУКОВОДИТЕЛЬ ЮЛ	Владелец подписи - СОТРУДНИК ЮЛ	Владелец подписи – ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ	Владелец подписи - ФИЗИЧЕСКОЕ ЛИЦО
<p>Надлежащим образом заверенные копии:</p> <p>1) свидетельство о регистрации юридического лица/ свидетельство о внесении записи в Единый государственный реестр юридических лиц (наличие ОГРН);</p> <p>2) свидетельство о постановке на учет в налоговом органе;</p> <p>3) 1 и 2 стр. Устава, либо выписка из ЕГРЮЛ (наличие юр. адреса и наименования организации);</p> <p>4) актуальный протокол общего собрания участников (решения) о назначении руководителя организации;</p> <p>5) паспорт владельца электронной подписи (разворот 2 и 3 страниц, а также страница с отметкой о регистрации по месту жительства);</p> <p>6) СНИЛС владельца электронной подписи;</p> <p>7) протокол собрания/решения/изменения к уставу, если были какие изменения в учредительных документах (смена юр. адреса, смена правовой формы)</p>	<p>Надлежащим образом заверенные копии:</p> <p>1) свидетельство о регистрации юридического лица/ свидетельство о внесении записи в Единый государственный реестр юридических лиц (наличие ОГРН);</p> <p>2) свидетельство о постановке на учет в налоговом органе;</p> <p>3) 1 и 2 стр. Устава, либо выписка из ЕГРЮЛ (наличие юр. адреса и наименования организации);</p> <p>4) актуальный протокол общего собрания участников (решения) о назначении руководителя организации;</p> <p>5) паспорт владельца электронной подписи (разворот 2 и 3 страниц, а также страница с отметкой о регистрации по месту жительства);</p> <p>6) СНИЛС владельца электронной подписи;</p> <p>7) протокол собрания/решения/изменения к уставу, если были какие изменения в учредительных документах (смена юр. адреса, смена правовой формы) регистрации юридического;</p> <p>8) приказ о назначении на должность владельца сертификата.</p>	<p>Надлежащим образом заверенные копии:</p> <p>1) свидетельство о постановке на учет в налоговом органе;</p> <p>2) свидетельство о регистрации физического лица в качестве индивидуально предпринимателя;</p> <p>3) паспорт владельца электронной подписи (разворот 2 и 3 страниц, а также страница с отметкой о регистрации по месту жительства);</p> <p>4) СНИЛС владельца электронной подписи.</p>	<p>Нотариально заверенные копии:</p> <p>1) свидетельство о постановке на учет в налоговом органе (ИНН физ. лица);</p> <p>2) паспорт владельца электронной подписи (разворот 2 и 3 страниц, а также страница с отметкой о регистрации по месту жительства);</p> <p>3) СНИЛС владельца электронной подписи.</p>
<p>Оригиналы:</p> <p>1) паспорт (руководителя/доверенного лица);</p> <p>2) заявление на выпуск электронной подписи;</p> <p>3) доверенности по форме ООО «КОРУС Консалтинг СНГ» (при прибытии в Удостоверяющий центр доверенного лица заявителя);</p> <p>4) печать организации (при прибытии в Удостоверяющий центр руководителя).</p>	<p>Оригиналы:</p> <p>1) паспорт (сотрудника/доверенного лица);</p> <p>2) заявление на выпуск электронной подписи;</p> <p>3) доверенности по форме ООО «КОРУС Консалтинг СНГ» (при прибытии в Удостоверяющий центр доверенного лица заявителя, в том числе владельца электронной подписи).</p>	<p>Оригиналы:</p> <p>1) паспорт (руководителя/доверенного лица);</p> <p>2) заявление на выпуск электронной подписи;</p> <p>3) доверенности по форме ООО «КОРУС Консалтинг СНГ» (при прибытии в Удостоверяющий центр доверенного лица заявителя);</p> <p>4) печать организации (при прибытии в Удостоверяющий центр руководителя)</p>	<p>Оригиналы:</p> <p>1) паспорт (сотрудника/доверенного лица);</p> <p>2) заявление на выпуск электронной подписи;</p> <p>3) нотариальная доверенность на право представления интересов владельца сертификата (при прибытии в Удостоверяющий центр доверенного лица заявителя);</p> <p>4) либо оригиналы вышеперечисленных копий.</p>

ФОРМА

Приложение № 4
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.**Доверенность №**

Дата выдачи «___» _____ 20__ года

Доверенность действительна по «___» _____ 20__ года

Я, _____
Фамилия Имя Отчество
_____ действующий на основании
_____ должность, название и ИНН организации _____ Устава, Положения

(далее – Заявитель (Клиент УЦ ООО «КОРУС Консалтинг СНГ»))

Я, _____
Фамилия Имя Отчество _____ должность, название организации

Паспорт: серия _____ № _____

Кем выдан: _____ Даты выдачи: _____

(далее – Владелец сертификата)

Доверяем:

_____ Фамилия Имя Отчество
Паспорт: серия _____ № _____

Кем выдан: _____ Даты выдачи: _____

(далее – Уполномоченное лицо)

представлять интересы Клиента (Заявителя) и/или Владельца сертификата в отношениях с Удостоверяющим центром ООО «КОРУС Консалтинг СНГ» с правом совершения следующих действий:

- вместо Владельца сертификата присутствовать при создании ключей электронной подписи и запроса на сертификат ключа проверки электронной подписи;
- вместо Владельца сертификата получить сертификат ключа проверки электронной подписи на бумажном носителе и ознакомиться под расписку от имени Заявителя с информацией, содержащейся в таком сертификате;
- вместо Владельца сертификата получить руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
- расписаться от имени Клиента в актах сдачи-приемки оказанных услуг и/или приема-передачи прав и в товарной накладной на токен;
- вместо Владельца сертификата получить ключевой носитель, содержащий:
 - ключевые файлы в контейнере;
 - сертификат ключа проверки электронной подписи;
- получение следующих материальных ценностей (выбрать необходимое):
 - Токен ESMART Token 64K в количестве _____ (_____) штук;
 - Токен Rutoken 32K s в количестве _____ (_____) штук;
 - Токен Rutoken 64K s в количестве _____ (_____) штук;
 - Лицензия на право использования «КриптоПро CSP» версия _____ на одном рабочем месте, бессрочная _____ (_____) штук;
 - Лицензия на право использования службы «КриптоПро OCSP Client» бессрочная _____ (_____) штук
 - Лицензия на право использования службы «КриптоПро TSP Client» бессрочная _____ (_____) штук
 - Лицензия на право использования «КриптоАРМ Стандарт» версия 5 бессрочная _____ (_____) штук

Полномочия по данной доверенности не могут быть передоверены другим лицам.

Подпись лица, получившего доверенность _____
_____ подпись _____ ФИО

Удостоверяем

_____ Должность Владельца сертификата _____
_____ подпись _____ ФИО
«___» _____ 20__ г.

_____ Должность руководителя _____
_____ подпись _____ ФИО
М.П. «___» _____ 20__ г.

ФОРМА

Приложение № 5
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.

**Заявление на аннулирование
квалифицированного сертификата ключа проверки электронной подписи
или на аннулирование такого сертификата**

_____ 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 __, свидетельство о регистрации в качестве ИП №__ от «__» ____ 20__ г.) (при необходимости)

просит прекратить, приостановить действие квалифицированного сертификата ключа проверки электронной подписи или аннулировать такой сертификат в соответствии с Федеральным законом № 63-ФЗ от 06.04.2011 «Об электронной подписи» и настоящим Регламентом, содержащего следующие идентификационные данные:

Серийный (уникальный) номер квалифицированного сертификата	
Дата начала действия квалифицированного сертификата	
ОГРН ЮЛИП	
Фамилия, имя и отчество владельца сертификата	
Продолжительность приостановления действия сертификата (заполняется при приостановлении)	с «___» _____ 20__ г. по «___» _____ 20__ г.
Основание аннулирования квалифицированного сертификата (заполняется при аннулировании)	
Иная информация о владельце сертификата (контактный адрес электронной почты)	

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

_____ Должность руководителя или уполномоченного
сотрудника ЮЛИП (при наличии)

_____ подпись

_____ Ф.И.О.

МП (при наличии)

«___» _____ 20__
г.

Отметки Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:

Заявление принял и проверил на полноту и достоверность данных:

_____ / _____ / «___» _____ 20__ г.
(Должность) (Подпись) (ФИО) (Дата)

ФОРМА

Приложение № 6
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.

**Заявление на получение информации о статусе
квалифицированного 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 квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КОРУС Консалтинг СНГ» и содержащего следующие идентификационные данные:

Серийный (уникальный) номер квалифицированного 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 ¹	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 (при наличии)

_____ подпись

_____ Ф.И.О.

МП (при наличии)

« ____ » _____ 20__ г.

Отметки Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:

Заявление принял и проверил на полноту и достоверность данных:

_____ (Должность)

_____ (Подпись)

/ _____ / (ФИО)

« ____ » _____ 20__ г.
(Дата)

¹ Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

ФОРМА

Приложение № 7
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «___» _____ 20__ г.Заявление на проверку подлинности электронной подписи
в электронном документе

_____ 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 в электронном документе 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 (при наличии)

_____ подпись

_____ Ф.И.О.

МП (при наличии)

«___» _____ 20__ г.

Отметки Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»:

Заявление принял и проверил на полноту и достоверность данных:

_____ (Должность)

_____ (Подпись)

/ _____ / (ФИО)

«___» _____ 20__ г. (Дата)

Приложение № 8
к Регламенту Удостоверяющего центра
ООО «КОРУС Консалтинг СНГ»
от «_____» _____ 20__ г.

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи.
 - 1.1. Обеспечить конфиденциальность ключей электронных подписей.
 - 1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.
 - 1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
 - 1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (если такие ограничения были установлены).
 - 1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
 - 1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата в Удостоверяющий центр по момент времени официального уведомления об аннулировании сертификата, либо об отказе в аннулировании.
 - 1.7. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
2. Порядок применения средств квалифицированной электронной подписи
 - 2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи, размещенной на сайте <http://www.esphere.ru/support/> в разделе «Удостоверяющий центр», либо на сайте производителя, в т.ч не разглашать содержимое носителей ключевой информации и/или не передавать сами носители лицам, к ним не допущенным, не выводить ключевую информацию на дисплей, принтер и иные средства отображения информации, а также не записывать на ключевые носители постороннюю информацию и т.д.
 - 2.2. Для предотвращения заражения компьютера с установленными средствами квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.
 - 2.3. В помещениях владельцев средств квалифицированной электронной подписи для хранения выданных им носителей ключей электронной подписи, эксплуатационной и технической документации, устанавливающих средства квалифицированной электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих владельцев средств квалифицированной электронной подписи.
 - 2.4. Заявителем Удостоверяющего центра соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств квалифицированной ЭП, назначены должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств; средства квалифицированной ЭП и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах.

Настоящее Руководство получено: _____ / _____ /
(подпись) (ФИО)

« _____ » _____ 20__ г.