РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «ИНФОРМАЦИОННЫЙ ЦЕНТР»

Редакция № 5

Москва 2020

СОДЕРЖАНИЕ

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Акционерное общество «Информационный центр», именуемое в дальнейшем «Удостоверяющий центр» зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1047796615349 от 19.08.2004 г., выдано Межрайонной инспекцией МНС России №46 по г. Москве. Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании Приказа Минкомсвязи России № 657 от 14.12.2016 г. «Об аккредитации удостоверяющих центров», на основании Свидетельства об аккредитации удостоверяющего центра, регистрационный № 694 от 14.12.2016 и на основании следующих лицензий:

– Лицензии ЛСЗ № 0015726 от 14 августа 2018 г. выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя). Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности»: работы, предусмотренные пунктами 12, 13, 14, 15, 20, 21, 22, 23, 24, 25, 26, 27, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложение к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313;

– Лицензия Федеральной службы по надзору в сфере связи № 130268 от 15 июля 2015 г. на право предоставления телематических услуг связи.

Реквизиты АО «Информационный центр»:
Полное наименование: Акционерное общество «Информационный центр»
Юридический адрес: 127410, г. Москва, Алтуфьевское ш., д. 37, корп. 1
Фактический адрес: 127410, г. Москва, Алтуфьевское ш., д. 37, корп. 1
Банковские реквизиты:
– ПАО РОСБАНК Г. МОСКВА
– БИК 044525256
– р/с 40702810397240000095
– к/с 30101810000000000256
ИНН/КПП: 7701553038 / 771501001
ОГРН: 1047796615349
Код по ОКВЭД: 62.09
Код по ОКПО: 73878489
Контактные телефоны, факс, адрес электронной почты:
Тел./Факс +7 (499) 455-17-25
Эл. почта: info@infc.ru
Адрес в сети Интернет: www.infc.ru

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Регламенте используются термины и определения, установленные Федеральным законом № 63-ФЗ «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

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

2.1.2 Сертификат ключа проверки электронной подписи (далее – СКПЭП) - квалифицированный сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом № 63-ФЗ «Об электронной подписи» и иным принимаемым в соответствии с ним нормативными правовыми актами и созданный аккредитованным удостоверяющим центром.

2.1.3 Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи. Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи) если:

– наступил момент времени начала действия ключа электронной подписи;

– срок действия ключа электронной подписи не истек;

– сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует на указанный момент времени.

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

2.1.5 Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра.

Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

2.1.6 Пользователь Удостоверяющего центра (далее - Пользователь УЦ) – физическое лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец ключа проверки электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами. Владельцем такого сертификата ключа проверки электронной подписи признается юридическое лицо, информация о котором содержится в таком сертификате. При этом распорядительным актом юридического лица определяется физическое лицо, ответственное за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами. В случае отсутствия указанного распорядительного акта лицом, ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, является руководитель юридического лица. В случае возложения федеральным законом полномочий по исполнению государственных функций на конкретное должностное лицо ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при исполнении государственных функций является это должностное лицо.

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

2.1.8 Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром или доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. Сертификат ключа проверки электронной подписи действует на определенный момент времени (действующий сертификат) если:

– наступил момент времени начала действия сертификата ключа проверки электронной подписи;

– срок действия сертификата ключа проверки электронной подписи не истек;

– сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие.

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

2.1.10 Служба актуальных статусов сертификатов – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого подписываются квалифицированной электронной подписью и предоставляются Пользователям УЦ электронные ответы, содержащие информацию о статусе сертификатов, выданных Удостоверяющим центром.

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

2.1.12 Специалист Удостоверяющего центра (далее – Специалист УЦ) – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по обеспечению создания ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, аннулирование, прекращение действия) сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром заверять копии сертификатов ключей проверки электронной подписи на бумажном носителе, выданных Удостоверяющим центром.

2.1.13 Список аннулированных сертификатов (далее - САС) – электронный документ с квалифицированной электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы, действие которых прекращено.

2.1.14 Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

2.1.15 Удостоверяющий центр – АО «Информационный центр», осуществляет выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи». Удостоверяющий центр с момента аккредитации уполномоченным федеральным органом исполнительной власти Российской Федерации в сфере использования электронной подписи осуществляет создание и выдачу квалифицированных сертификатов ключей проверки электронной подписи, а также сертификатов для участников государственных (муниципальных) закупок.

2.1.16 Уполномоченное лицо Удостоверяющего центра – лицо, наделенное полномочиями выполнять проверку документов либо их надлежащим образом заверенных копий, подтверждающих достоверность информации, представляемой заявителем для включения в СКПЭП на предмет их соответствия требованиям Регламента Удостоверяющего центра; устанавливать факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно представляет, а также факт отсутствия явных признаков подделки документов, а также идентифицировать личность физических лиц, обращающихся в Удостоверяющий центр за изготовлением СКПЭП.

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

2.1.18 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.

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

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

3. СТАТУС РЕГЛАМЕНТА

3.1. Регламент Удостоверяющего центра АО «Информационный центр», именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров и определяет порядок создания и управления квалифицированными сертификатами ключей проверки электронной подписи.

3.2. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

3.3. Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно−технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

3.4. Настоящий Регламент распространяется:

– в форме электронного документа на Сайте Удостоверяющего центра адресу: https://infc.ru

– в форме документа на бумажном носителе при подаче Заявления о выпуске Сертификата.

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Присоединение к Регламенту.

4.1.1 Присоединение к настоящему Регламенту осуществляется путем заключения Договора на оказание услуг Удостоверяющего центра или в момент предоставления заинтересованным лицом Заявления на изготовление сертификата ключа проверки электронной подписи по форме Приложения №1.

4.1.2 С момента получения Удостоверяющим центром документов, необходимых для изготовления сертификата ключа проверки электронной подписи лицо, подавшее Заявление на изготовление сертификата ключа проверки электронной подписи (документы), считается присоединившимся к Регламенту и является Стороной Регламента.

4.1.3 Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления о присоединении к Регламенту в случаях, предусмотренных действующим законодательством.

4.1.4 Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения, вносимые в Регламент, в соответствии с условиями настоящего Регламента.

4.1.5 После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения на срок действия Договора на оказание услуг Удостоверяющего центра.

4.2. Порядок расторжения Регламента.

4.2.1 Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

– по собственному желанию одной из Сторон;

– нарушения одной из Сторон условий настоящего Регламента.

4.2.2 В случае расторжения Регламента инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за тридцать календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения Сторонами своих обязательств и проведения взаиморасчетов.

4.2.3 Расторжение Регламента влечет за собой автоматическое расторжение Договора об оказании услуг Удостоверяющего центра.

4.2.4 Прекращение действия Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

4.3. Изменение Регламента.

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

4.3.2 Уведомление о внесении изменений в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений на Сайте Удостоверяющего центра.

4.3.3 Все изменения, вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными с момента размещения указанных изменений в Регламенте на Сайте Удостоверяющего центра.

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

4.3.5 Любые изменения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений в силу. В случае несогласия с изменениями Сторона Регламента имеет право до вступления в силу таких изменений на расторжение Регламента в порядке, предусмотренном п. 4.2. настоящего Регламента.

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

4.4. Применение Регламента.

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

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

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

5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

5.1. Удостоверяющий центр осуществляет свою деятельность в качестве аккредитованного Удостоверяющего центра на основании решения Минкомсвязи России, являющегося федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. С информацией по аккредитации Удостоверяющего центра Сторона, присоединившаяся к Регламенту, может ознакомиться на официальном сайте Минкомсвязи России.

5.2. Удостоверяющий центр осуществляет свою деятельность в соответствии с лицензиями ФСБ России на право осуществления технического обслуживания шифровальных (криптографических) средств, распространения шифровальных (криптографических) средств, оказания услуг в области шифрования информации.

5.3. Для изготовления сертификата ключа проверки электронной подписи Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить Удостоверяющему центру следующие документы, либо их надлежащим образом, заверенные копии и (или) сведения из них:

– основной документ, удостоверяющий личность;

– номер страхового свидетельства государственного пенсионного страхования (СНИЛС) заявителя - физического лица;

– идентификационный номер налогоплательщика-заявителя - физического лица;

– основной государственный регистрационный номер заявителя - юридического лица;

– основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя;

– свидетельство о государственной регистрации - юридического лица;

– номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

- документ, подтверждающий право заявителя действовать от имени юридического лица без доверенности либо подтверждающий право заявителя действовать от имени государственного органа или органа местного самоуправления;

– Заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи.

5.4. Ответственность за подлинность предоставляемых документов и достоверность содержащейся в них информации несут Заявители. Ответственность за соответствие документам сведений, указанных в

заявлении, несет Заявитель. В случае необходимости Удостоверяющий Центр оставляет за собой право требовать иные документы, необходимые для полной идентификации Пользователя УЦ.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1. Обязанности Удостоверяющего центра. Удостоверяющий центр обязан:

6.1.1 Предоставить Пользователю УЦ сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

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

6.1.3 Использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им сертификатов ключей проверки электронной подписи и САС.

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

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

6.1.6 Обеспечить уникальность идентификационных данных Пользователей УЦ, заносимых в сертификаты ключей проверки электронной подписи.

6.1.7 Создать сертификат ключа проверки электронной подписи Пользователя УЦ по заявлению на создание сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

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

6.1.9 Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Пользователей УЦ.

6.1.10 Обеспечить сохранение в тайне созданного ключа электронной подписи Пользователя УЦ.

6.1.11 Прекратить действие сертификата ключа проверки электронной подписи Пользователя УЦ по соответствующему заявлению на прекращение (аннулирование) действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.12 Прекратить действие сертификата ключа проверки электронной подписи Пользователя УЦ в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи Пользователя УЦ.

6.1.13 Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в т. ч. сети "Интернет", к реестру квалифицированных сертификатов этого аккредитованного удостоверяющего центра в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

6.1.14 Официально уведомить о прекращении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации САС.

Публиковать актуальный САС на сайте Удостоверяющего центра: http://cdp.infc.ru/cdp/ao2012_cdp.crl

Публиковать актуальный реестр квалифицированных сертификатов на сайте Удостоверяющего центра: http://aia.informcenter.ru/aia/aia.crt

Период публикации САС – 7 (семь) суток.

6.2. Обязанности Стороны, присоединившейся к Регламенту. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1 С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу https://infc.ru/docs/reglament_ao_ic.pdf за сведениями об изменениях в Регламенте.

6.3. Обязанности Пользователя Удостоверяющего центра. Пользователь Удостоверяющего центра обязан:

6.3.1 Обеспечить конфиденциальность ключей электронных подписей и принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

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

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

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

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

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

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

6.3.8 Не использовать ключ ЭП до предоставления УЦ подписанной копии сертификата ключа проверки ЭП, соответствующего данному ключу ЭП.

6.4. Права Удостоверяющего центра. Удостоверяющий центр имеет право:

6.4.1 Отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае ненадлежащего оформления заявления на создание сертификата ключа проверки электронной подписи.

6.4.2 Отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае непредоставления и/или ненадлежащего предоставления документов, предусмотренных настоящим Регламентом.

6.4.3 Отказать в прекращении действия сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления соответствующего заявления на прекращение (аннулирование) действия сертификата ключа проверки электронной подписи.

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

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

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

6.4.7 В одностороннем порядке прекращать действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра, если Удостоверяющему центру стало известно, что владелец сертификата ключа проверки электронной подписи не владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате.

6.5. Права Пользователя Удостоверяющего центра. Пользователь Удостоверяющего центра имеет право:

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

6.5.2 Применять САС ключей проверки электронных подписей, созданный Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

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

6.5.4 Получить копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Удостоверяющим центром.

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

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут ответственность в соответствии с действующим законодательством РФ. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

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

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

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

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к Регламенту.

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

8.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

8.4. Сторона, получившая от другой Стороны претензию, обязана в течение 30 (тридцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

8.5. Спорные вопросы между Сторонами, не урегулированные в претензионном порядке, решаются в Арбитражном суде г. Москвы.

9. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

9.1. Создание сертификата ключа проверки электронной подписи. Удостоверяющий центр осуществляет регистрацию пользователей и создание квалифицированных сертификатов ключей проверки электронной подписи только тем лицам, которые присоединились к настоящему Регламенту и являются Стороной настоящего Регламента, а также при соблюдении Пользователем Удостоверяющего центра финансовых и других условий соответствующего договора. Под регистрацией пользователей понимается внесение регистрационной информации о пользователях в реестр Удостоверяющего Центра. Создание квалифицированного сертификата ключа проверки электронной подписи осуществляется на основании заявления на создание квалифицированного сертификата ключа проверки электронной подписи. Форма заявления на изготовление квалифицированного сертификата ключа проверки электронной подписи приведена в Приложении № 1 (А, Б, В) настоящего Регламента. Заявление на изготовление сертификата ключа проверки электронной подписи должно содержать данные, установленные Статьей 17 63-ФЗ «Об электронной подписи». К данному заявлению должны прилагаться все необходимые документы, которые подтверждают вносимые в сертификат данные. В случае создания квалифицированного сертификата ключа проверки электронной подписи юридическому лицу наряду с указанием в сертификате наименования юридического лица должно указываться физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица. Если ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи юридического лица будут использоваться для автоматического создания электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и

принимаемыми в соответствии с ними нормативными правовыми актами, то физическое лицо может не указываться в сертификате ключа проверки электронной подписи. Получение сформированного Удостоверяющим центром квалифицированного сертификата ключа проверки электронной подписи может быть осуществлено физическим лицом, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата.

Специалист либо иное уполномоченное лицо Удостоверяющего центра выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по основному документу, удостоверяющему личность. Заявитель под расписку знакомится с информацией из сертификата ключа проверки электронной подписи. Услуги Удостоверяющего центра считаются оказанными, если Заявитель не предъявит претензий в письменном виде по их качеству и объему в течение 5 (пяти) рабочих дней со дня их оказания, с обязательным предварительным уведомлением Удостоверяющего центра о выставлении претензии по телефону, электронной почте или с использованием других средств связи. Одновременно с выдачей квалифицированного сертификата владельцу квалифицированного сертификата выдается руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

9.2. Прекращение действия квалифицированного сертификата ключа проверки электронной подписи. Удостоверяющий центр прекращает действие квалифицированного сертификата ключа проверки электронной подписи Пользователя УЦ в следующих случаях:

– при прекращении действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту, по усмотрению Удостоверяющего центра;

– если не подтверждено, что владелец квалифицированного сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

– если установлено, что содержащийся в таком квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате ключа проверки электронной подписи;

– если вступило в силу решение суда, которым, в частности, установлено, что квалифицированный сертификат ключа проверки электронной подписи содержит недостоверную информацию;

– по заявлению владельца квалифицированного сертификата ключа проверки электронной подписи;

– в связи с аннулированием квалифицированного сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу.

– по истечении срока действия квалифицированного сертификата ключа проверки электронной подписи;

– при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан квалифицированный сертификат ключа проверки электронной подписи.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) CAC, содержащего сведения о сертификате, действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем прекращения действия сертификата ключа проверки электронной подписи признается время внесения записи об этом в реестр сертификатов. Информация о размещении CAC заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point квалифицированного сертификата ключа проверки электронной подписи. В случае прекращения действия квалифицированного сертификата ключа проверки электронной подписи по истечению срока его действия временем прекращения действия квалифицированного сертификата ключа проверки электронной подписи признается время, хранящееся в поле notAfter поля Validity квалифицированного сертификата ключа проверки электронной подписи. В этом случае информация о сертификате, действие которого прекращено, в CAC не заносится. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра временем прекращения действия квалифицированного сертификата ключа проверки электронной подписи Пользователя УЦ признается время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, фиксирующееся Удостоверяющим центром. При этом информация о квалифицированном сертификате ключа проверки электронной подписи Пользователя УЦ в CAC не заносится.

9.3. Прекращение действия квалифицированного сертификата ключа проверки электронной подписи по заявлению его владельца. Подача заявления в Удостоверяющий центр на прекращение действия квалифицированного сертификата ключа проверки электронной подписи может быть осуществлена лично или посредством ФГУП Главный центр специальной связи по форме Приложения № 2 (А, Б, В) настоящего Регламента. После получения Удостоверяющим центром заявления на прекращение действия квалифицированного сертификата ключа проверки электронной подписи Специалист УЦ осуществляет его рассмотрение и обработку. Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона "Об электронной подписи", или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений.. В случае отказа в прекращении действия квалифицированного сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа. При принятии положительного решения Специалист УЦ осуществляет прекращение действия квалифицированного сертификата ключа проверки электронной подписи.

9.4. Получение информации о статусе квалифицированного сертификата ключа проверки электронной подписи. Получение информации о статусе квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется на основании заявления Стороны, присоединившейся к Регламенту. Данное заявление оформляется по форме Приложения № 4 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи. Заявление должно содержать следующую информацию:

– дата и время подачи заявления;

– время и дата (либо период времени), на момент наступления которых требуется установить статус квалифицированного сертификата ключа проверки электронной подписи;

– идентификационные данные владельца, статус квалифицированного сертификата ключа проверки электронной подписи которого требуется установить;

– серийный номер квалифицированного сертификата ключа проверки электронной подписи, статус которого требуется установить.

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

Предоставление заявителю справки о статусе квалифицированного сертификата ключа проверки электронной подписи должно быть осуществлено не позднее 20 (Двадцати) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

9.5. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени.

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе квалифицированных сертификатов ключей проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого квалифицированного сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием квалифицированного сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

– выполнены условия признания квалифицированной электронной подписи в OCSP-ответе;

– квалифицированная электронная подпись в OCSP-ответе сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы актуальных статусов сертификатов.

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – http://aia.informcenter.ru/aia/aia.crt

10. ФОРМА СЕРТИФИКАТА КЛЮЧА ПОДПИСИ, САС И СРОКИ ДЕЙСТВИЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ

10.1. Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром. Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи». Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи может быть занесено:

– поле Subject (идентифицирует владельца сертификата);

– поле E (Email) – адрес электронной почты;

– поле T (Title) – должность полномочного представителя юридического лица, данные которого занесены в сертификат наряду с наименованием юридического лица (если владелец сертификата – юридическое лицо);

– расширение Private Key Validity Period – срок действия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи, следующего формата:

– действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;

– действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;

– расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) – набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с сертификатом ключа проверки электронной подписи (если такие ограничения установлены);

– расширение CRL Distribution Point (Точка распространения САС) – набор адресов точек распространения САС;

иные поля и расширения по усмотрению Удостоверяющего центра.

10.2. Форма САС (CRL) Удостоверяющего центра.

Название	**Описание**	**Содержание**
Базовые поля САС		
Version	Версия	V2
Issuer	Издатель САС	Идентификационные данные УЦ
thisUpdate	Время издания САС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен САС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	САС	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки события, повлекшего прекращение или приостановление действия сертификата 3. Код причины прекращения действия сертификата (Reson Code): "0" - Не указана; "1" - Компрометация ключа (нарушение конфиденциальности

Название	Описание	Содержание
		ключа); "2" - Компрометация ЦС (нарушение конфиденциальности ключа Удостоверяющего центра; "3" - Изменение принадлежности; "4" - Сертификат заменен; "5" - Прекращение работы; "6" - Приостановление действия
signatureAlgorithm	Алгоритм электронной подписи	ГОСТ Р 34.11/34.10-2001
signatureAlgorithm	Алгоритм электронной подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя CAC	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя CAC	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения CAC		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего центра, на котором подписан CAC
SzOID_CertSrv_C A_Version	Объектный идентификатор сертификата издателя	Версия сертификата Удостоверяющего Центра

10.3. Срок действия сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи Удостоверяющего центра не превышает 5 (Пять) лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно. Срок действия сертификата ключа проверки электронной подписи Пользователя УЦ не превышает 15 (пятнадцать) месяцев. Время начала периода действия сертификата ключа подписи Пользователя УЦ и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

11. ФОРС-МАЖОР

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

11.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства, включая военные действия,

массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

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

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

11.5. Неизвещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства. В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

12. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

12.1. Типы конфиденциальной информации:

12.1.1 Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре.

12.1.2 Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

12.2. Типы информации, не являющейся конфиденциальной:

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

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

12.2.3 Информация, включаемая в сертификаты ключей подписи и САС, издаваемые Удостоверяющим центром, не считается конфиденциальной.

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

13. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» разработана «Политика в отношении обработки персональных данных АО «Информационный центр», которая размещена на сайте УЦ по адресу https://infc.ru/docs/politica.pdf

13.2. Владелец СКПЭП дает свое согласие на обработку персональных данных в момент предоставления Заявления на изготовление сертификата ключа проверки электронной подписи.

14. СПИСОК ПРИЛОЖЕНИЙ

ПРИЛОЖЕНИЕ №1А. Заявление для юридических лиц на изготовление квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №1Б. Заявление для индивидуальных предпринимателей на изготовление квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №1В. Заявление для физических лиц на изготовление квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №2А. Заявление для юридических лиц на прекращение действия квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №2Б. Заявление для индивидуальных предпринимателей на прекращение действия квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №2В. Заявление для физических лиц на прекращение действия квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №3Б. Заявление для индивидуальных предпринимателей на прекращение действия квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №3В. Заявление для физических лиц на прекращение действия квалифицированного сертификата ключа проверки электронной подписи (СКПЭП).

ПРИЛОЖЕНИЕ №4. Заявление на получение информации о статусе сертификата ключа подписи.

ПРИЛОЖЕНИЕ №5. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

ЛИСТ ПРЕДЫДУЩИХ РЕДАКЦИЙ

№ п/п	Наименование	Дата
1.	Редакция № 1	01.11.16
2.	Редакция № 2	17.02.17
3.	Редакция № 3	21.09.18
4.	Редакция № 4	02.04.19
5.	Редакция № 5	31.07.20
6.		
7.		
8.		
9.		

ПРИЛОЖЕНИЕ №1А
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №1А. ЗАЯВЛЕНИЕ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ НА ИЗГОТОВЛЕНИЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

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

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

действующего на основании _____
(основание полномочий)

просит создать ключ электронной подписи и сертификат ключа проверки электронной подписи уполномоченного представителя в соответствии с указанными в настоящем заявлении идентификационными данными*:

Фамилия Имя Отчество		
Адрес электронной почты		
Телефон		
Должность/Звание		
Наименование подразделения		
Краткое наименование организации		
ИНН/ОГРН	ИНН	ОГРН
Юридический адрес		
Область		
Страна	RU	
Паспорт	(серия)	(номер)
	(кем и когда выдан)	
СНИЛС		

*В соответствии с Федеральным законом от 27.07.06 г. № 152-ФЗ «О персональных данных», выражаю свое согласие на обработку моих персональных данных, включающих: фамилию, имя, отчество, место работы, должность, и иные сведения, необходимые для исполнения целей по регистрации и обслуживанию. В процессе оказания мне услуг удостоверяющим центром АО «Информационный центр» я предоставляю право осуществлять все действия (операции) с моими персональными данными, включая передачу таких данных третьим лицам в соответствии с законодательством, сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

М.П.

Руководитель организации _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_г.

ПРИЛОЖЕНИЕ №1Б
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №1Б. ЗАЯВЛЕНИЕ ДЛЯ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ НА ИЗГОТОВЛЕНИЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

_____

(полное наименование индивидуального предпринимателя)

_____

просит создать ключ электронной подписи и сертификат ключа проверки электронной подписи уполномоченного представителя в соответствии с указанными в настоящем заявлении идентификационными данными*:

Фамилия Имя Отчество		
Адрес электронной почты		
Телефон		
ИНН/ОГРНИП	ИНН	ОГРНИП
Юридический адрес		
Область		
Страна	RU	
Паспорт	(серия)	(номер)
	(кем и когда выдан)	
СНИЛС		

*В соответствии с Федеральным законом от 27.07.06 г. № 152-ФЗ «О персональных данных», выражаю свое согласие на обработку моих персональных данных, включающих: фамилию, имя, отчество, место работы, должность, и иные сведения, необходимые для исполнения целей по регистрации и обслуживанию. В процессе оказания мне услуг удостоверяющим центром АО «Информационный центр» я предоставляю право осуществлять все действия (операции) с моими персональными данными, включая передачу таких данных третьим лицам в соответствии с законодательством, сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

М.П.**

**в случае, если индивидуальный предприниматель работает без печати, печать не ставится

ПРИЛОЖЕНИЕ №1В
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №1В. ЗАЯВЛЕНИЕ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ
НА ИЗГОТОВЛЕНИЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

_____

(полные фамилия имя отчество владельца СКПЭП)

_____

просит создать ключ электронной подписи и сертификат ключа проверки электронной подписи уполномоченного представителя в соответствии с указанными в настоящем заявлении идентификационными данными*:

Фамилия Имя Отчество		
Адрес электронной почты		
Телефон		
ИНН	ИНН	
Адрес по месту регистрации		
Область		
Страна	RU	
Паспорт	(серия)	(номер)
	(кем и когда выдан)	
СНИЛС		

*В соответствии с Федеральным законом от 27.07.06 г. № 152-ФЗ «О персональных данных», выражаю свое согласие на обработку моих персональных данных, включающих: фамилию, имя, отчество, место работы, должность, и иные сведения, необходимые для исполнения целей по регистрации и обслуживанию. В процессе оказания мне услуг удостоверяющим центром АО «Информационный центр» я предоставляю право осуществлять все действия (операции) с моими персональными данными, включая передачу таких данных третьим лицам в соответствии с законодательством, сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

АО «Информационный центр»
Введено в действие 31.07.2020года

ПРИЛОЖЕНИЕ №2А
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №2А. ЗАЯВЛЕНИЕ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ
НА ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

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

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

действующего на основании _____
(основание полномочий)

в связи с _____
(причина прекращения действия)

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

Серийный номер сертификата ключа подписи		
Краткое наименование организации		
ИНН/ОГРН	(ИНН)	(ОГРН)
Фамилия, Имя, Отчество владельца СКПЭП		
Должность		
СНИЛС		

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

М.П.

Руководитель организации _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_г.

ПРИЛОЖЕНИЕ №2Б
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №2Б. ЗАЯВЛЕНИЕ ДЛЯ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ НА ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

_____
(полное наименование индивидуального предпринимателя)

в связи с _____
(причина прекращения действия)

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

Серийный номер сертификата ключа подписи		
Фамилия Имя Отчество владельца СКПЭП		
ИНН/ОГРНИП	(ИНН)	(ОГРНИП)
СНИЛС		

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

М.П.*

*в случае, если индивидуальный предприниматель работает без печати, печать не ставится.

ПРИЛОЖЕНИЕ №2В
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №2В. ЗАЯВЛЕНИЕ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ
НА ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

_____
(полные фамилия имя отчество владельца СКПЭП)

в связи с

_____
(причина прекращения действия)

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

Серийный номер сертификата ключа подписи	
Фамилия Имя Отчество владельца СКПЭП	
ИНН	(ИНН)
СНИЛС	

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

АО «Информационный центр»
Введено в действие 31.07.2020года

ПРИЛОЖЕНИЕ №4
к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №4. ЗАЯВЛЕНИЕ №_____
ДЛЯ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ, ЮРИДИЧЕСКИХ ЛИЦ, ФИЗИЧЕСКИХ ЛИЦ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СТАТУСЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (СКПЭП)

_____
(полное наименование организации, включая организационно-правовую форму, либо ФИО ФЛ, в том числе ИП-заявителя)

в лице _____
(должность, ФИО руководителя или организации-заявителя, либо ФИО ФЛ, в том числе ИП-заявителя)

действующего на основании _____
(основание полномочий)

просит предоставить информацию о статусе квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром АО «Информационный центр» и содержащего следующие данные:

Серийный номер СКПЭП		
Краткое наименование организации		
ИНН/ОГРН/ОГРНИП	(ИНН)	(ОГРН/ОГРНИП)
Фамилия, Имя, Отчество владельца СКПЭП		
Должность		
СНИЛС		

Время (период времени) на момент наступления которого требуется установить статус СКПЭП: с «_____» по «_____».
(дата, время) (дата, время)

Владелец СКПЭП _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_ г.

М.П.

Руководитель организации _____/_____ /
(подпись) (фамилия, инициалы)

«___» _____ 202_г.

ПРИЛОЖЕНИЕ №5

к Регламенту Удостоверяющего центра АО «Информационный центр»

ПРИЛОЖЕНИЕ №5. РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (ДАЛЕЕ - КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ)	– сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром
СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ	– шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи
СПАМ	– рассылка коммерческой и иной рекламы или иных видов сообщений (информации) лицам, не выражавшим желания их получать
ХАКЕРСКАЯ АТАКА	– действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо ее дестабилизация, либо отказ в обслуживании
АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	– специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом

ОБЯЗАННОСТИ ВЛАДЕЛЬЦА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

1. Обеспечить конфиденциальность ключей электронных подписей.
2. Ограничьте доступ к компьютеру, который используется для работы с ключевой информацией и подписания документов электронной подписью. Исключите бесконтрольный доступ в помещения, в которых размещаются средства электронной подписи.
3. Не оставляйте личный ключевой носитель и/или PIN-код доступа к нему без присмотра.
4. Обеспечьте безопасное хранение ключей электронной подписи на ключевом носителе в сейфе или запираемом ящике стола.
5. Подсоединяйте ключевой носитель к компьютеру только для подписания электронных документов, и в обязательном порядке извлекайте его из компьютера сразу после окончания работы. Блокируйте компьютер и извлекайте ключевые носители при уходе с рабочего места.
6. Не извлекайте ключевой носитель во время его работы, т.к. это может привести к потере данных на нем.
7. Не допускается снимать несанкционированные копии с ключевых носителей, передавать ключевые носители лицам, к ним не допущенным.
8. Используйте на компьютере только лицензионное программное обеспечение. Своевременно устанавливайте обновления безопасности операционной системы.
9. Применять для формирования электронной подписи только действующий ключ электронной подписи.
10. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.
11. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи, либо в случае утраты личного ключевого носителя и/или PIN-кода доступа к нему.
12. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
13. 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.

ПОРЯДОК ПРИМЕНЕНИЯ СРЕДСТВ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

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.
2. Если вам в течение сеанса работы со средствами ЭП приходится многократно использовать ключевой носитель, то для ускорения работы используйте настройку криптопровайдера «Запомнить пароль». После завершения сеанса работы обязательно удалите запомненные пароли, для чего используйте возможности криптопровайдера.
3. 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.
4. В организации должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств квалифицированной электронной подписи, назначены владельцы средств квалифицированной электронной подписи и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств.