УТВЕРЖДАЮ

Управляющий

ЗАО «ТаксНет»

_____/М.М. Гайфуллин

«__» июня 2017 год

РЕГЛАМЕНТ

Удостоверяющего центра ЗАО «ТаксНет»

Казань

2017

1. Общие положения.

1.1. Сведения об Удостоверяющем центре

Закрытое акционерное общество «ТаксНет», именуемое далее «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Казани. Свидетельство о регистрации № 2966/К (50–02) выдано 27.07.2001 г. Государственной регистрационной палатой при Министерстве юстиции Республики Татарстан. Свидетельство о внесении записи в Единый государственный реестр юридических лиц за основным государственным регистрационным номером 1021602855262 от 12.12.2002 г.

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании следующих разрешительных документов:

- Приказа Минкомсвязи России № 191 от 06.08.2012.г. «Об аккредитации удостоверяющих центров»;
- Лицензии ФСБ России, рег. № 296Н от 14 октября 2013 г., на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Лицензии Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации, серия КИ 0226, номер 011374, регистрационный номер 0537 от 21 ноября 2006 года.

Реквизиты ЗАО «ТаксНет»:

Полное наименование: Закрытое акционерное общество «ТаксНет»

Сокращенное наименование: ЗАО «ТаксНет»

Юридический адрес: 420021, г. Казань, ул. Каюма Насыри, д.28, офис 1010

Фактический адрес: 420021, г. Казань, ул. Каюма Насыри, д.28, офис 1010

Адрес для корреспонденции: 420021, г. Казань, ул. Каюма Насыри, д.28, офис 1010

Банковские реквизиты (наименование банка, БИК, ИНН, р/с, к/с):

- Филиал «Нижегородский» АО «Альфа-банк» г. Нижний Новгород
- БИК 042202824
- Р/с 40702810929070000106
- К/с 30101810200000000824

ИНН/КПП: 1655045406/165501001

ОГРН: 1021602855262

Код по ОКВЭД: 62.01

Код по ОКПО: 57234965

1.2. Контактные данные Удостоверяющего центра

Заявители и владельцы сертификатов могут получить информацию о предоставляемых услугах, их стоимости, вопросам использования электронной подписи и средств электронной подписи по следующим каналам связи:

- Единая служба продаж: 8-800-333-80-89
- Служба работы с абонентами: 8-800-333-86-12
- Техническая поддержка: (843) 231-92-00
- Факс: (843) 231-92-01; (843) 231-92-07
- E-mail: office@taxnet.ru, udc@taxnet.ru

Адреса, график работы, справочные телефоны Центров выдачи Удостоверяющего центра опубликованы на сайте http://taxnet.ru.

1.3. Предмет регулирования Регламента

1.3.1. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации и определяет порядок и сроки предоставления услуг Удостоверяющего центра, включая права, обязанности, ответственность Сторон, принятые форматы данных, основные организационно-технические мероприятия, направленные на обеспечение деятельности Удостоверяющего центра.

Настоящий Регламент распространяется:

- в форме электронного документа по адресу: http://taxnet.ru/download/uc_reglament.pdf;
- в форме документа на бумажном носителе при подаче Заявления о присоединении к Регламенту за вознаграждение, установленное прайс-листом Удостоверяющего центра.

1.4. Порядок применения Регламента

1.4.1. Присоединение к Регламенту.

Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр заявления о присоединении к Регламенту по форме Приложений № 1.а-1.в. настоящего Регламента.

С момента регистрации заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее заявление, считается присоединившимся к Регламенту и является Стороной Регламента.

Удостоверяющий центр вправе отказать любому лицу в приёме и регистрации заявления о присоединении к Регламенту по обоснованным мотивам, к которым относятся:

- представленное заявление не соответствует форме, установленной настоящим Регламентом;

- сведения в заявлении не соответствуют сведениям, указанным в документах, представленных вместе с заявлением;
- отсутствие соответствующих полномочий у лица, представившего заявление.

Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении к Регламенту в Удостоверяющем центре. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения, вносимые в Регламент, в соответствии с условиями настоящего Регламента.

После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения на неопределённый срок.

1.4.2. Расторжение Регламента.

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.

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 согласно условиям Регламента. Действие всех сертификатов, владельцем которых является Сторона, присоединившаяся к Регламенту, по усмотрению Удостоверяющего центра может быть прекращено.

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).

1.4.3. Изменения (дополнения) Регламента

Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений на сайте Удостоверяющего центра по адресу – http://taxnet.ru/download/uc_reglament.pdf.

Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении одного месяца с даты размещения указанных изменений (дополнений) в Регламенте на сайте Удостоверяющего центра по адресу - http://taxnet.ru/download/uc_reglament.pdf.

Все изменения (дополнения), 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.

Любые изменения (дополнения) в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений в силу. В случае несогласия с изменениями Сторона Регламента имеет право до вступления в силу таких изменений на расторжение Регламента в порядке, предусмотренном п.1.4.2. настоящего Регламента.

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

1.5. Стоимость услуг Удостоверяющего центра. Сроки и порядок расчетов

1.5.1. Удостоверяющий центр осуществляет свою деятельность на коммерческой основе. Стоимость и перечень услуг Удостоверяющего центра определяются Прайс-листом, который публикуется на сайте Удостоверяющего центра по адресу - http://taxnet.ru. Оплата услуг Удостоверяющего центра производится Стороной, присоединившейся к Регламенту, на условиях полной предоплаты в течение 5 (пяти) банковских дней с момента получения выставленного счета.

1.5.2. Удостоверяющий центр безвозмездно предоставляет:

- сертификаты в форме электронных и бумажных документов из реестра сертификатов Удостоверяющего центра;
- информацию из реестра отозванных сертификатов.

1.5.3. Удостоверяющий центр безвозмездно осуществляет:

- аннулирование, приостановление/возобновление действия сертификата;
- создание сертификатов, вызванных внеплановой сменой ключей электронной подписи владельца сертификата по причине нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра;
- выписку из реестра сертификатов, в том числе информацию об аннулировании сертификата.

1.5.4. Оказание услуг производится на основании договора публичной оферты, опубликованного на сайте http://taxnet.ru/company/docs.

1.6. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

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

Усиленная неквалифицированная электронная подпись (НЭП) – электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;
3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
4) создается с использованием средств электронной подписи.

Усиленная квалифицированная электронная подпись (КЭП) – электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;
2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

Квалифицированный сертификат ключа проверки электронной подписи (сертификат КЭП) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об Электронной подписи» 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. В настоящем Регламенте термин «сертификат» применяется для обозначения как сертификата КЭП, так и сертификата НЭП.

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

Заявитель – физическое или юридическое лицо, независимо от организационно-правовой формы, а также иной хозяйствующий субъект, обратившееся в Удостоверяющий центр за получением сертификата.

Доверенное лицо заявителя – физическое лицо, выступающее от имени заявителя, уполномоченное передать в Удостоверяющий центр документы на выпуск сертификата и получить сертификат.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

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.

Средства электронной подписи (средства ЭП) – 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. Средства электронной подписи должны соответствовать требованиям, утвержденными Приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. N 796 г. Москва "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра".

Средства удостоверяющего центра (средства УЦ) – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра. Средства УЦ должны соответствовать требованиям, утвержденными Приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. N 796 г. Москва "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра".

Участники электронного взаимодействия – государственные органы, органы местного самоуправления, организации, граждане, осуществляющие обмен информацией в электронной форме.

Маркер временного доступа – идентификатор и секретный пароль, представляющиеся заявителю для формирования и предоставления в Удостоверяющий центр запроса на выпуск сертификата посредством специального программного обеспечения Удостоверяющего центра.

Доверенное лицо Удостоверяющего центра (доверенное лицо) – физическое лицо, являющееся сотрудником Центра выдачи и наделенное Удостоверяющим центром полномочиями по вручению маркеров временного доступа или сертификатов, созданных Удостоверяющим центром.

Вручение маркера временного доступа или сертификата – передача заявителю доверенным лицом Удостоверяющего центра маркера временного доступа или сертификата. При вручении маркера временного доступа или сертификата доверенное лицо обязано установить личность заявителя, либо полномочия лица, выступающего от имени заявителя.

Подтверждение владения ключом электронной подписи – получение удостоверяющим центром доказательств того, что лицо, обратившееся за получением сертификата, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, подписанный собственноручной подписью сотрудника удостоверяющего центра или доверенного лица удостоверяющего центра и заверенный печатью Удостоверяющего центра. Содержательная часть копии сертификата соответствует содержательной части сертификата ключа проверки электронной подписи.

ПАКМ «КриптоПро HSM» (ПАКМ) – программно-аппаратный криптографический модуль, разработанный в соответствии с «Требованиями к шифровальным

(криптографическим) средствам и предназначенный для защиты информации не содержащей сведений, составляющих государственную тайну», и удовлетворяет классу защиты КВ2 данных требований (при выполнении "Правил пользования ПАКМ «КриптоПро HSM». ЖТЯИ.00046-01 90 02" в части условий применения и «Руководства Администратора безопасности» ЖТЯИ.00046-01 90 03). ПАКМ позволяет организовать централизованное хранение и управление ключами пользователей УЦ. При этом секретные ключи пользователей формируются и хранятся в ПАКМ в зашифрованном виде.

Секретный ключ доступа к ПАКМ (ключ доступа) - взаимодействие любого приложения на рабочих станциях пользователей или серверах с СКЗИ ПАКМ «КриптоПро HSM» через посредника – «Клиента HSM» с использованием технологического ключа доступа, формируемого на ПАКМ.

Пользователь ПАКМ – владелец ключа доступа к ПАКМ «КриптоПро HSM». Пользователь ПАКМ имеет право удаленного доступа к криптографическим функциям ПАКМ.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 8:30 до 17:30 (время московское) каждого дня недели за исключением выходных и праздничных дней.

Реестр выданных сертификатов – реестр выданных Удостоверяющим центром сертификатов, включающий в себя информацию, содержащуюся в выданных сертификатах.

Реестр отозванных сертификатов – электронный документ с электронной подписью Удостоверяющего центра, создаваемый на определенный момент времени и включающий в себя список серийных номеров сертификатов, действие которых аннулировано, прекращено или приостановлено.

Сертификат ключа проверки электронной подписи Удостоверяющего центра (сертификат Удостоверяющего центра) – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи Удостоверяющего центра в изготовленных им сертификатах ключей проверки электронной подписи и списках отозванных сертификатов.

Удостоверяющий центр (УЦ) – ЗАО «ТаксНет», осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи». Удостоверяющий центр с момента аккредитации уполномоченным федеральным органом исполнительной власти Российской Федерации в сфере использования электронной подписи (Министерство связи и массовых коммуникаций Российской Федерации) осуществляет изготовление, выдачу и управление сертификатами.

Центр выдачи – юридическое лицо или индивидуальный предприниматель, действующие на основании агентского договора с Удостоверяющим центром и отвечающие положениям федерального законодательства на осуществление лицензируемой деятельности в области шифрования информации.

2. Перечень функций и услуг Удостоверяющего центра

В процессе осуществления деятельности Удостоверяющий центр предоставляет заявителям и владельцам сертификатов следующие услуги:

- создание и выдача сертификатов заявителям, обратившимся за их получением, при условии установления личности заявителя, либо полномочий лица, выступающего от имени заявителя;
- установление сроков действия сертификатов;
- изготовление копий сертификатов на бумажных носителях;
- создание ключей электронной подписи и ключей проверки электронной подписи с записью их на ключевой носитель;
- проверка уникальности ключей проверки электронной подписи в реестре сертификатов;
- предоставление сертификатов в электронной или бумажной форме, находящихся в реестре выданных сертификатов по запросам заявителей и владельцев сертификатов;
- прекращение действия и аннулирование сертификатов по запросам их владельцев и в иных случаях, установленных Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также настоящим Регламентом. Результат оказания услуги – внесение сведений о прекращении действия или об аннулировании сертификата в реестр отозванных сертификатов;
- приостановление и возобновление действия сертификатов по обращениям их владельцев;
- предоставление сведений об аннулированных сертификатах и сертификатах, действие которых прекращено, путем публикации реестра отозванных сертификатов по адресам, указанным в расширении CRL (Certificate Revocation List) сертификата;
- выдача средств электронной подписи, сертифицированных в соответствии с правилами сертификации Российской Федерации, содержащих ключ электронной подписи и ключ проверки электронной подписи, или обеспечивающих возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- проверка подлинности электронной подписи в электронном документе;
- предоставление прав на использование программ для ЭВМ, необходимых для управления сертификатами на условиях простой (неисключительной) лицензии;
- выдача руководства по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи;
- информирование заявителей о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

Дополнительно заявители и владельцы сертификатов могут получить услуги по установке и настройке средств электронной подписи и консультацию по вопросам применения сертификатов в различных информационных системах.

3. Права и обязанности сторон

3.1. Права Удостоверяющего центра

В соответствии со статьями 13 и 15 Федерального закона от 06.04.2011г. № 63-ФЗ «Об Электронной подписи» Удостоверяющий центр имеет право:

- запрашивать у заявителя документы для подтверждения информации, содержащейся в заявлении на создание и выдачу сертификата;
- 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 государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем;
- запрашивать и получать из государственных информационных ресурсов:
    1) выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;
    2) выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;
    3) выписку из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации;
- в случае наличия противоречий между сведениями, представленными заявителем и сведениями, полученными из государственных информационных ресурсов, запрашивать у заявителя дополнительные документы, подтверждающие полномочия заявителя и достоверность представленных им сведений;
- не принимать у заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации, а также не соответствующие требованиям информационных систем, на которых планируется применение сертификата;
- отказать заявителю в создании и выдаче сертификата в случае оформления заявления на создание и выдачу сертификата с ошибками, наличия исправлений, подчисток, приписок, не подтвержденных собственноручной подписью заявителя или его доверенного лица;
- отказать заявителю в создании сертификата в случае не предоставления и/или ненадлежащего предоставления документов, установленных п. 5.1, п. 5.3 настоящего Регламента;
- отказать заявителю в выдаче сертификата в случае невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об Электронной подписи» и принимаемыми в соответствии с ним нормативными правовыми актами;
- отказать заявителю в создании и выдаче сертификата в случае, если им предоставлен ключевой носитель, не удовлетворяющий требованиям информационной системы, в которой будет применяться сертификат;
- отказать заявителю в создании и выдаче сертификата в случае наличия у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности маркера временного доступа;
- отказать владельцу сертификата в аннулировании, приостановлении и возобновлении действия сертификата в случае ненадлежащего оформления соответствующего заявления на аннулирование, приостановление и возобновление

действия сертификата, а также в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям;

- прекратить действие сертификата без заявления владельца 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 всех сведений, занесенных в данный сертификат. Удостоверяющий центр уведомляет владельца сертификата о свих намерениях посредством отправки сообщения на электронный адрес владельца сертификата;
- приостановить действие сертификата, а также восстановить действие ранее приостановленного сертификата в соответствии с п. 5.6, п. 5.7 настоящего Регламента.

3.2. Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

- вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;
- обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечивать круглосуточную доступность реестра сертификатов в информационно-телекоммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания;
- обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей;
- информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;
- при выдаче сертификата КЭП ознакомить заявителя под расписку с информацией, содержащейся в сертификате КЭП и выдать руководство по обеспечению безопасности использования КЭП и средств КЭП;
- направить сертификат КЭП на регистрацию в Единую систему идентификации и аутентификации сведения в соответствии с пунктом 5 статьи 18 Федерального закона от 06.04.2011 года № 63-ФЗ «Об Электронной подписи»;
- предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата;
- 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;

- отказать заявителю в создании сертификата в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата;
- использовать для создания ключа электронной подписи Удостоверяющего центра и формирования электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- 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;
- использовать для создания и управления сертификатами средства Удостоверяющего центра, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- организовать свою работу по московскому времени, синхронизировать по времени все свои программные и технические средства обеспечения деятельности;
- создать сертификат по заявлению на создание и выдачу сертификата, в соответствии с порядком, определенным в настоящем Регламенте;
- предоставить заявителю сертификат Удостоверяющего центра в электронной форме;
- использовать ключ электронной подписи удостоверяющего центра только для подписи издаваемых им сертификатов и списков отозванных сертификатов;
- принимать меры по защите ключа электронной подписи Удостоверяющего центра от несанкционированного доступа;
- обеспечить уникальность серийных номеров создаваемых сертификатов;
- обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах;
- обеспечивать конфиденциальность созданных ключей электронных подписей;
- прекратить действие (аннулировать), приостановить и возобновить действие сертификата по соответствующему заявлению владельца сертификата на аннулирование, приостановление и возобновление действия сертификата, в соответствии с порядком, определенным настоящим Регламентом;
- прекратить действие сертификата, если истек установленный срок, на который действие данного сертификата было приостановлено;
- прекратить действие сертификата в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был изготовлен сертификат;
- официально уведомить о прекращении действия (аннулировании), приостановлении и возобновлении действия сертификатов всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации реестра отозванных сертификатов на сайте Удостоверяющего центра по адресу - http://ca.taxnet.ru;

- обеспечивать круглосуточную доступность реестра сертификатов в информационно-телекоммуникационной сети Интернет, за исключением планового или внепланового технического обслуживания.

3.3. Права заявителей и владельцев сертификатов

3.3.1. Права заявителей:

- обратиться в удостоверяющий центр с заявлениями на выполнение Удостоверяющим центром действий, установленных настоящим Регламентом;
- обратиться за получением средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- получить в электронной форме списки отозванных сертификатов, выпущенных Удостоверяющим центром;
- применять список отозванных сертификатов для установления статусов сертификатов, созданных Удостоверяющим центром;
- получить в электронной форме сертификаты, содержащиеся в реестре выданных сертификатов Удостоверяющего центра;
- получить в электронной форме сертификаты Удостоверяющего центра;
- обратиться в Удостоверяющий центр с заявлением на предоставление возможности использования сервисов служб Удостоверяющего центра, определенных Прайс-листом Удостоверяющего центра.

3.3.2. Права владельцев сертификатов.

Владельцы сертификатов обладают правами заявителей и дополнительно имеют право:

- применять для хранения ключа электронной подписи ключевой носитель, поддерживаемый средством электронной подписи, или использовать ПАКМ «КриптоПро HSM», расположенный на территории Удостоверяющего центра;
- получить копию сертификата на бумажном носителе, заверенную Удостоверяющим центром;
- обращаться в Удостоверяющий центр для аннулирования, приостановления действия, возобновления действия своего сертификата в течении срока действия соответствующего ключа электронной подписи.

3.3.3. Обязанности заявителей:

- ознакомиться с положениями настоящего Регламента и договора публичной оферты;
- своевременно оплачивать услуги по созданию и выдаче сертификата;
- использовать для создания и проверки электронных подписей, изготовления ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- предоставлять достоверную и актуальную на момент обращения в Удостоверяющий центр информацию, необходимую для создания и выдачи сертификата;

- обеспечить конфиденциальность маркера временного доступа. В случае утери реквизитов маркера временного доступа, обратиться в Центр выдачи и отозвать действие выданного маркера временного доступа.

3.3.4. Обязанности владельцев сертификатов.

Владельцы сертификатов имеют обязанности заявителей и дополнительно обязаны:

- обеспечить не реже одного раза в тридцать календарных дней гарантированное ознакомление с полным текстом изменений настоящего Регламента, публикуемых на сайте Удостоверяющего центра по адресу - http://taxnet.ru/download/uc_reglament.pdf, до вступления их в силу;
- известить Удостоверяющий центр об изменениях в учредительных и идентификационных документах в течение 5-ти рабочих дней с момента регистрации изменений;
- обеспечить конфиденциальность ключей электронных подписей;
- применять для создания электронной подписи только действующий ключ электронной подписи;
- использовать для создания электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- использовать КЭП в соответствии с ограничениями, содержащимися в сертификате КЭП (если такие ограничения установлены);
- не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр для прекращения действия соответствующего сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- не использовать ключ электронной подписи, связанный с сертификатом, заявление на аннулирование 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 о прекращении действия сертификата, либо об отказе в прекращении действия;
- не использовать ключ электронной подписи, связанный с сертификатом, заявление на приостановление действия которого подано в Удостоверяющий центр в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия;
- не использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого приостановлено.

4. Порядок и сроки предоставления услуг Удостоверяющим центром

4.1. Процедура создания ключей электронной подписи

Заявитель может создать ключ электронной подписи и ключ проверки электронной подписи одним из способов:

- самостоятельно на своем рабочем месте с использованием сертифицированных средств электронной подписи, маркера временного доступа, полученного в Центре выдачи, и программного обеспечения, предоставляемого Удостоверяющим центром;
- в Удостоверяющем центре. Создание ключей производится на автоматизированном рабочем месте Удостоверяющего центра, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, в присутствии заявителя. Ключ электронной подписи, созданный таким образом, записывается Удостоверяющим центром на ключевой носитель, который выдаётся заявителю или его доверенному лицу по окончании процедуры выдачи сертификата.

Факт создания Удостоверяющим центром ключа электронной подписи и соответствующего ему ключа проверки электронной подписи, содержащегося в сертификате, или факт создания данных ключей заявителем самостоятельно при помощи сертифицированных средств электронной подписи, подтверждает факт владения владельца сертификата ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате.

4.2. Сроки действия ключевых документов

4.2.1. Сроки действия ключевых документов Удостоверяющего центра.

Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени изготовления ключа электронной подписи Удостоверяющего центра.

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

4.2.2. Сроки действия ключевых документов владельца сертификата.

Срок действия ключа электронной подписи заявителя устанавливается эксплуатационной документацией на средство электронной подписи, с использованием которого такой ключ создается. Начало периода действия ключа электронной подписи заявителя исчисляется с момента начала действия сертификата, соответствующего данному ключу.

Срок действия сертификата заявителя, равен сроку действия ключа электронной подписи, соответствующего данному сертификату. Время начала периода действия

сертификата заявителя и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

4.3. Порядок плановой смены ключей электронной подписи Удостоверяющего центра

4.3.1. Плановая смена ключа электронной подписи Удостоверяющего центра и соответствующего ему сертификата КЭП.

Процедура плановой смены ключей Удостоверяющего центра выполняется в период действия ключа электронной подписи удостоверяющего центра и осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ электронной подписи, соответствующий ему ключ проверки электронной подписи и запрос на выдачу сертификата КЭП Удостоверяющего центра в формате PKSC#10 Base-64;
- Удостоверяющий центр направляет сформированный запрос на выдачу сертификата КЭП в адрес Головного удостоверяющего центра Федерального органа исполнительной власти, уполномоченного в сфере использования электронной подписи (уполномоченный орган);
- уполномоченный орган с использованием средств головного удостоверяющего центра создает сертификат КЭП, выдает его Удостоверяющему центру и публикует в реестре выданных сертификатов;
- Удостоверяющий центр устанавливает полученный сертификат КЭП на средства удостоверяющего центра.

  Удостоверяющий центр использует КЭП, основанную на сертификате КЭП, выданном ему головным удостоверяющим центром, только для подписания сертификатов КЭП.

Старый ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, создаваемых Удостоверяющим центром.

Владельцы сертификатов уведомляются о смене ключей электронной подписи Удостоверяющего центра путем рассылки соответствующего уведомления по электронной почте и публикации информации на официальных сайтах Удостоверяющего центра (http://taxnet.ru) и уполномоченного органа (http://e-trust.gosuslugi.ru).

4.3.2. Плановая смена ключа электронной подписи Удостоверяющего центра и соответствующего ему сертификата, который используется для подписания от имени удостоверяющего центра сертификатов НЭП.

Процедура плановой смены ключей удостоверяющего центра выполняется в период действия ключа электронной подписи удостоверяющего центра и осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр создает новый сертификат Удостоверяющего центра.

Владельцы сертификатов уведомляются о смене ключей электронной подписи Удостоверяющего центра путем рассылки соответствующего уведомления по

электронной почте и публикации информации на официальном сайте Удостоверяющего центра http://taxnet.ru.

Старый ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, создаваемых Удостоверяющим центром.

4.4. Порядок внеплановой смены ключей электронной подписи Удостоверяющего центра

Процедура внеплановой смены ключей удостоверяющего центра выполняется в случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра.

4.4.1. Внеплановая смена ключа электронной подписи Удостоверяющего центра и соответствующего ему сертификата КЭП.

- Удостоверяющий центр уведомляет уполномоченный орган о наступлении события, повлекшего компрометацию ключа электронной подписи;
- Уполномоченный орган с использованием средств головного удостоверяющего центра аннулирует сертификат КЭП;
- Удостоверяющий центр получает новый сертификат КЭП в соответствии с порядком из пункта 4.3.1. настоящего Регламента.

Владельцы сертификатов уведомляются о внеплановой смене ключа электронной подписи Удостоверяющего центра путем рассылки соответствующего уведомления по электронной почте, публикации информации на официальном сайте Удостоверяющего центра http://taxnet.ru и публикации реестра отозванных сертификатов уполномоченным органом.

Все действовавшие на момент нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификаты, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

Реестр отозванных сертификатов подписывается старым ключом электронной подписи (подвергшимся процедуре внеплановой смены).

После получения официального уведомления о факте внеплановой смены ключей Удостоверяющего центра владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых сертификатов в соответствии с пунктом 5.4 настоящего Регламента.

Удостоверяющий центр безвозмездно создает сертификаты для всех владельцев сертификатов, чьи сертификаты прекратили свое действие в связи с внеплановой заменой.

4.4.2. Внеплановая смена ключа электронной подписи Удостоверяющего центра и соответствующего ему сертификата, который используется для подписания от имени удостоверяющего центра сертификатов НЭП, выполняется в соответствии с пунктом 4.3.2. настоящего Регламента.

Владельцы сертификатов уведомляются о внеплановой смене ключа электронной подписи Удостоверяющего центра путем рассылки соответствующего уведомления по электронной почте, публикации информации на официальном сайте Удостоверяющего центра http://taxnet.ru.

Все действовавшие на момент нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификаты, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

Реестр отозванных сертификатов подписывается старым ключом электронной подписи (подвергшимся процедуре внеплановой смены).

После получения официального уведомления о факте внеплановой смены ключей Удостоверяющего центра владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых сертификатов в соответствии с пунктом 5.4 настоящего Регламента.

4.5. Порядок осуществления Удостоверяющим центром смены ключей электронной подписи владельца сертификата

Данный процесс предполагает подачу заявления на создание и выдачу сертификата как в письменной форме на бумажном носителе, так и в форме электронного документа, подписанного КЭП.

Если смена ключа владельца сертификата связана с его компрометацией или угрозой компрометации, то заявление на создание и выдачу сертификата подается в письменной форме на бумажном носителе при личном прибытии заявителя или его доверенного лица в Удостоверяющий центр. Процедура создания ключа электронной подписи осуществляется в соответствии с пунктом 5.4. настоящего Регламента.

4.5.1. Смена ключа электронной подписи в связи с наступлением сроков окончания действия сертификата.

4.5.1.1. Заявитель подает заявление на создание и выдачу сертификата в электронной форме с помощью программного обеспечения, предоставляемого Удостоверяющим центром. Заявление на создание и выдачу сертификата в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве подписываемых данных запрос на сертификат в формате PKCS#10 и подписанный электронной подписью с использованием ключа электронной подписи и сертификата КЭП, владельцем которых является заявитель.

4.5.1.2. Владелец сертификата на данном этапе идентифицируется по значениям атрибутов поля Subject сертификата.

4.5.1.3. Созданный сертификат, заверенный электронной подписью Удостоверяющего центра, предоставляется его владельцу в виде файла. Создание сертификата и выдача сертификата осуществляются Удостоверяющим центром в течение 3-х (трех) рабочих дней с момента получения запроса на создание сертификата.

4.5.1.4. После получения сертификата владелец сертификата с помощью программного обеспечения Удостоверяющего центра производит его установку на своем рабочем месте.

4.5.1.5. Электронные документы, подписанные КЭП владельца, хранятся в электронном архиве Удостоверяющего центра.

4.5.1.6. Удостоверяющий центр производит регистрацию сертификата КЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона от 06.04.2011г. № 63-ФЗ «Об Электронной подписи».

5. Процедура создания и выдачи сертификатов

Удостоверяющий центр осуществляет создание сертификатов только тем лицам, которые присоединились к настоящему Регламенту и являются стороной настоящего Регламента.

Удостоверяющий центр осуществляет создание сертификата на основании заявления на создание и выдачу сертификата ключа проверки электронной подписи. Форма заявления приведена в Приложениях № 2.а-2.в к настоящему Регламенту.

5.1. Требования к заявлению на создание и выдачу сертификата

5.1.1. Заявление заполняется лично заявителем на компьютере или вручную на русском языке печатными буквами. Фамилия, имя и отчество заявителя указываются полностью на основании документа, удостоверяющего личность. Должность указывается в соответствии со штатным расписанием. Заявление подписывается собственноручной подписью заявителя.

5.1.2. Заявление не должно содержать ошибок, подчисток, исправлений, приписок не подтвержденных собственноручной подписью заявителя или его доверенного лица.

5.1.3. Заявление должно содержать все реквизиты документа: печать (если предусмотрена), подписи, даты.

5.1.4. На заявлении должны хорошо просматриваются сведения, подлежащие внесению в сертификат.

5.1.5. В случае подачи заявления представителем юридического лица, заявление заверяется подписью руководителя и печатью организации.

5.1.6. Заявление на создание и выдачу сертификата может быть оформлено в письменной форме на бумажном носителе, или в форме электронного документа, подписанного КЭП владельца сертификата.

5.2. Порядок установления личности заявителя

Удостоверяющий центр устанавливает личность заявителя (доверенного лица заявителя) в следующем порядке:

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

5.3. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи сертификата

Заявитель или доверенное лицо заявителя представляет в Удостоверяющий центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности заявителя (доверенного лица заявителя), а также документы, подтверждающие сведения, на основании которых Удостоверяющим центром вносятся сведения в сертификат.

Перечень документов зависит от категории заявителя.

5.3.1. Перечень документов для юридических лиц:

- свидетельство о государственной регистрации юридического лица - копия, заверенная подписью руководителя и печатью юридического лица, либо нотариально;
- свидетельство о внесении записи о юридическом лице в Единый государственный реестр юридических - копия, заверенная подписью руководителя и печатью юридического лица, либо нотариально;
- свидетельство о постановке на учет в налоговом органе – копия, заверенная подписью руководителя и печатью юридического лица, либо нотариально;
- устав организации - копия, заверенная подписью руководителя и печатью юридического лица, либо нотариально;
- приказ (протокол) о назначении руководителя организации – оригинал или копия, заверенная руководителем организации;
- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность - для тех лиц, которые указываются в сертификатах наряду с указанием наименования юридического лица. Оригиналы или копии, заверенные подписью руководителя и печатью юридического лица, либо нотариально;
- страховое свидетельство государственного пенсионного страхования владельца сертификата – оригинал или копия, заверенная подписью руководителя и печатью юридического лица;
- иные документы, установленные настоящим Регламентом, а также дополнительные документы по усмотрению Удостоверяющего центра, к которым относятся:

5.3.2. Для индивидуальных предпринимателей:

- свидетельство о государственной регистрации в качестве индивидуального предпринимателя – заверенная индивидуальным предпринимателем (при наличии печати), либо нотариально;
- свидетельство о постановке на учет в налоговом органе физического лица по месту жительства в Российской Федерации – заверенная индивидуальным предпринимателем (при наличии печати), либо нотариально;
- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность - для тех лиц, которые указываются в сертификатах. Оригиналы или копии, заверенные индивидуальным предпринимателем (при наличии печати), либо нотариально;
- страховое свидетельство государственного пенсионного страхования владельца сертификата – оригинал или копия, заверенная индивидуальным предпринимателем (при наличии печати);
- иные документы, установленные настоящим Регламентом, а также дополнительные документы по усмотрению Удостоверяющего центра.

5.3.3. Для физических лиц:

- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность. Оригиналы или нотариально заверенные копии;
- страховое свидетельство государственного пенсионного страхования – оригинал или нотариально заверенная копия;
- свидетельство о постановке на учет в налоговом органе – оригинал или нотариально заверенная копия;
- иные документы, установленные настоящим Регламентом, а также дополнительные документы по усмотрению Удостоверяющего центра.

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

5.4. Порядок создания и выдачи сертификата

В случае создания сертификата 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 или доверенности. Доверенность должна предоставляться заявителем вместе с заявлением на создание и выдачу сертификата и быть действительной в течении всего срака действия сертификата. Допускается не указывать в качестве владельца сертификата физическое лицо, действующее от имени юридического лица, в сертификате, используемом для автоматического создания и (или) автоматической проверки 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. Владельцем такого сертификата признается юридическое лицо, информация о котором содержится в таком сертификате.

Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем, по данным, полученным из государственных информационных ресурсов:

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

Если сведения, полученные из государственных информационных ресурсов, подтверждают достоверность информации, представленной заявителем и установлена личность заявителя - физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением сертификата, Удостоверяющий центр выдает заявителю сертификат. В противном случае удостоверяющий центр отказывает заявителю в выдаче сертификата и возвращает заявителю документы.

Срок создания и выдачи сертификата не превышает 3-х (трех) рабочих дней с момента получения Удостоверяющим центром заявления на создание и выдачу сертификата.

5.4.1. Порядок создания сертификата с использованием маркера временного доступа, полученного в Центре выдачи.

Данный процесс предполагает подачу заявления на создание и выдачу сертификата в письменной форме на бумажном носителе.

5.4.1.1. Доверенное лицо принимает от заявителя документы, необходимые для создания и выдачи маркера временного доступа, устанавливает личность заявителя - физического лица, обратившегося за получением маркера временного доступа в соответствии с пунктом 5.2 настоящего Регламента, осуществляет проверку достоверности документов и сведений, представленных заявителем.

5.4.1.2. При положительных результатах проверки доверенное лицо формирует маркер временного доступа, распечатывает на бумажном носителе реквизиты маркера временного доступа, передает их заявителю или его доверенному лицу. Срок действия маркера временного доступа составляет 7 (семь) календарных дней.

5.4.1.3. В течение срока действия маркера временного доступа заявитель самостоятельно на своем рабочем месте, используя программное обеспечение Удостоверяющего центра, создает на ключевом носителе ключи электронной подписи, формирует и направляет в Удостоверяющий центр запрос на создание сертификата в электронной форме. Если в течение срока действия маркера временного доступа заявитель не направит в Удостоверяющий центр запрос на со3

5.4.1.4. здание сертификата, то он повторно обращается в Центр выдачи за получением нового маркера временного доступа. Центр выдачи осуществляет выдачу нового маркера временного доступа на возмездной основе на основании представленных на момент обращения в Центра выдачи комплекта документов.

5.4.1.5. Удостоверяющий центр получает запрос на создание сертификата, поданный заявителем в электронной форме, и принимает решение о создании и выдаче сертификата. Данные заявителя, содержащиеся в запросе на сертификат, должны совпадать с данными, указанными в заявлении на создание и выдачу сертификата. При несоблюдении этого условия Удостоверяющий центр отказывает в создании сертификата.

5.4.1.6. В случае отказа в создании сертификата заявитель уведомляется об этом с указанием причины отклонения запроса. При принятии положительного решения, Удостоверяющий центр создает сертификат. Созданный сертификат, заверенный электронной подписью Удостоверяющего центра, предоставляется его владельцу в виде файла, содержащего созданный сертификат в электронной форме. Создание сертификата и уведомление владельца осуществляются Удостоверяющим центром в течение 1 (одного) рабочего дня с момента получения запроса на создание сертификата.

5.4.1.7. После получения сертификата владелец сертификата с помощью программного обеспечения Удостоверяющего центра производит его установку на своем рабочем месте, формирует электронную копию

сертификата, подписывает электронной подписью и направляет в Удостоверяющий центр. Подписывая своей электронной подписью электронную копию сертификата, владелец ознакамливается и соглашается с информацией, содержащейся в сертификате.

5.4.1.8. Электронные документы, подписанные электронной подписью владельца, хранятся в электронном архиве Удостоверяющего центра.

5.4.1.9. Удостоверяющий центр производит регистрацию сертификата КЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона от 06.04.2011г. № 63-ФЗ «Об Электронной подписи».

5.4.2. Порядок создания сертификата при обращении заявителя или доверенного лица заявителя в Удостоверяющий центр.

Данный процесс предполагает подачу заявления на создание и выдачу сертификата заявителем или доверенным лицом заявителя в письменной форме на бумажном носителе.

5.4.2.1. Удостоверяющий центр принимает от заявителя документы, необходимые для создания и выдачи сертификата, устанавливает личность заявителя - физического лица, обратившегося за получением маркера временного доступа в соответствии с пунктом 5.2 настоящего Регламента, осуществляет проверку достоверности документов и сведений, представленных заявителем. В случае отказа в создании сертификата заявитель уведомляется об этом с указанием причины отказа. При принятии положительного решения, Удостоверяющий центр выполняет действия по созданию ключа электронной подписи и сертификата. Ключ электронной подписи и сертификат по согласованию с заявителем могут быть записаны на ключевой носитель или сгенерированы непосредственно в ПАКМ «КриптоПро HSM». К ключевому носителю могут предъявляться дополнительные требования со стороны информационной системы, в которой будет применяться сертификат. Ключевой носитель, предоставленный заявителем, должен быть проинициализированным (отформатированным), не содержать никакой информации, за исключением данных инициализации. Ключевые носители, не удовлетворяющие данным требованиями, не могут быть использованы Удостоверяющим центром для записи ключевой информации.

5.4.2.2. Удостоверяющий центр формирует ключи электронной подписи и сертификат. По окончании работ заявителю передаются:

- ключевой носитель, содержащий изготовленные ключи электронной подписи и сертификат;
- копия сертификата на бумажном носителе;
- карточка отзыва с ключевой фразой, которая в дальнейшем будет использована Удостоверяющим центром для аутентификации владельца сертификата при выполнении регламентных процедур;
- руководство по работе со средствами криптографической защиты информации.

5.4.2.3. При получении сертификата заявитель под расписку ознакамливается с информацией, содержащейся в сертификате и получает руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи. Факт выдачи ключей электронной подписи заносится в Журнал учета и выдачи ключевых документов.

5.4.2.4. Удостоверяющий центр производит регистрацию сертификата КЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона от 06.04.2011г. № 63-ФЗ «Об Электронной подписи».

5.5. Прекращение (аннулирование) сертификата

5.5.1. Удостоверяющий центр прекращает действие сертификата в следующих случаях:

- по заявлению владельца сертификата;
- при прекращении действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту, по усмотрению Удостоверяющего центра;
- по истечении срока, на который действие сертификата было приостановлено;
- по истечении срока действия сертификата;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был изготовлен сертификат;
- прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам.

5.5.2. Удостоверяющий центр аннулирует сертификат в следующих случаях:

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

5.5.3. Подача заявления на прекращение действия (аннулирование) сертификата осуществляется владельцем сертификата или его доверенным лицом в письменной форме на бумажном носителе. Прием заявлений осуществляется в Удостоверяющем центре и Центрах выдачи в рабочие дни.

5.5.4. Информация о прекращении действия или аннулировании сертификата вносится Удостоверяющим центром в реестр отозванных сертификатов в течение двенадцати часов с момента приема заявления на аннулирование сертификата, или наступления иного события, предусмотренного настоящим Регламентом. По требованию информационной системы, в которой планируется применение сертификата, могут быть установлены более короткие сроки внесения сертификата в реестр отозванных сертификатов.

5.5.5. Действие сертификата прекращается с момента публикации реестра отозванных сертификатов, в который внесен этот сертификат.

5.5.6. Адреса публикации реестра отозванных сертификатов заносятся в созданные Удостоверяющим центром сертификаты в расширение CRL Distribution Point сертификата.

5.5.7. В случае прекращения действия сертификата по истечению срока его действия, временем прекращения действия сертификата признается время, хранящееся в поле notAfter поля Validity сертификата. В этом случае информация о сертификате, действие которого прекращено, в реестр отозванных сертификатов не заносится.

5.5.8. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра временем прекращения действия сертификата признается время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, фиксирующееся Удостоверяющим центром. При этом информация о сертификате владельца в реестр отозванных сертификатов не заносится.

5.6. Приостановление действия сертификата

5.6.1. Удостоверяющий центр приостанавливает действие сертификата:

- по заявлению владельца сертификата;
- по заявке владельца сертификата в устной форме, в случае нарушения конфиденциальности или подозрения на нарушение конфиденциальности ключа электронной подписи;
- по собственной инициативе, если возникла необходимость проверить имеющуюся в распоряжении Удостоверяющего центра информацию об обстоятельствах, которые могут привести к прекращению действия сертификата.

5.6.2. Подача заявления на приостановление действия сертификата осуществляется владельцем сертификата или его доверенным лицом в письменной форме на бумажном носителе. Прием заявлений осуществляется в Удостоверяющем центре и Центрах выдачи в рабочие дни.

5.6.3. Подача заявки на приостановление действия сертификата в устной форме осуществляется владельцем сертификата исключительно при нарушении конфиденциальности ключа электронной подписи или подозрения в нарушении конфиденциальности ключа электронной подписи. Заявка подается владельцем сертификата по телефону. Владелец сертификата должен сообщить Удостоверяющему центру следующую информацию:

- идентификационные данные, содержащиеся в сертификате, действие которого необходимо приостановить;
- серийный номер сертификата, действие которого требуется приостановить;
- ключевую фразу (формируется Удостоверяющим центром и выдается на бумажном носителе вместе с копией сертификата).

Заявка на приостановление действия сертификата принимается Удостоверяющим центром только в случае положительной аутентификации владельца сертификата (совпадения ключевой фразы, сообщенной владельцем сертификата по телефону, и ключевой фразы, хранящейся в Удостоверяющем центре). Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата, владелец сертификата должен предоставить в Удостоверяющий центр заявление на прекращение действия сертификата (в том случае, если факт нарушения конфиденциальности ключа электронной подтвердился), либо заявление на

возобновление действия сертификата (в том случае, если нарушения конфиденциальности ключа электронной подписи не было). заявления подаются в письменной форме на бумажном носителе.

5.6.4. Информация о прекращении действия сертификата вносится удостоверяющим центром в реестр сертификатов в течение двенадцати часов с момента наступления указанных обстоятельств, или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата прекращается с момента публикации реестра отозванных сертификатов, в который внесен этот сертификат.

5.6.5. Адреса публикации реестра отозванных сертификатов заносятся в созданные Удостоверяющим центром сертификаты в расширение CRL (Certificate Revocation List) сертификата.

5.6.6. Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа проверки электронной подписи составляет 15 (Пятнадцать) дней. Максимальный - до окончания срока действия сертификата. Удостоверяющий центр может возобновить действие сертификата в течении срока, на который действие сертификата было приостановлено, если причины, по которым срок действия сертификата был приостановлен, устранены. По истечении срока, на который действие сертификата было приостановлено, сертификат прекращает своё действие.

5.6.7. После приостановления действия сертификата удостоверяющий центр сообщает владельцу сертификата о наступлении события, повлекшего приостановление действие сертификата, и уведомляет его о том, что действие сертификата приостановлено путем отправки сообщения на электронный адрес, указанный в сертификате. Срок, на который приостанавливается действия сертификата, не может быть больше срока действия сертификата, оставшегося с момента подачи заявления до окончания срока его действия.

5.7. Возобновление действия сертификата

5.7.1. Удостоверяющий центр возобновляет действие сертификата только по заявлению его владельца при выполнении следующих условий:

- действие сертификата было приостановлено;
- срок действия сертификата на момент обращения в Удостоверяющий центр не истек.

5.7.2. Подача заявления на возобновление действия сертификата может быть осуществлена владельцем сертификата или его доверенным лицом в письменной форме на бумажном носителе. Прием заявлений осуществляется в Центрах выдачи в рабочие дни. Срок рассмотрения заявления – не более 12-ти часов с момента его приема.

5.7.3. Удостоверяющий центр может отказать владельцу возобновить действие его сертификата при отсутствии у удостоверяющего центра подтверждений того, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате. В случае отказа в возобновлении действия сертификата Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

5.7.4. Информация о возобновлении действия сертификата вносится удостоверяющим центром в реестр выданных сертификатов в течение двенадцати часов с момента принятия решения о возобновлении действия сертификата. Действие сертификата возобновляется с момента изъятия серийного номера этого сертификата из реестра отозванных сертификатов.

5.8. Получение информации о статусе сертификата

5.8.1. Получение информации о статусе сертификата, созданного удостоверяющим центром, осуществляется на основании заявления стороны, присоединившейся к Регламенту. Заявление оформляется по форме Приложений № 8.а-8.в. настоящего Регламента и предоставляется в Удостоверяющий центр лично, либо посредством почтовой или 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 сертификата;
- идентификационные данные Владельца сертификата;
- серийный номер сертификата, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата, которая предоставляется заявителю.

5.8.2. Предоставление заявителю справки о статусе сертификата осуществляется не позднее 10 (Десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

5.9. Проверка подлинности электронной подписи в электронном документе

5.9.1. Удостоверяющий центр обеспечивает проверку подлинности электронной подписи в электронном документе в том случае, если формат представления электронного документа с электронной подписью соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS). Решение о соответствии формата представления электронного документа с электронной подписью стандарту CMS принимает Удостоверяющий центр.

5.9.2. Проверка подлинности электронной подписи в электронных документах осуществляется удостоверяющим центром на основании заявления стороны, присоединившейся к Регламенту. Заявление оформляется по форме Приложений № 9.а-9.в настоящего Регламента и предоставляется в Удостоверяющий центр лично, либо посредством почтовой или курьерской связи. Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные владельца сертификата, электронную подпись которого необходимо проверить в электронном документе;
- дата и время формирования электронной подписи электронного документа;
- дата и время, на момент наступления которых требуется проверить подлинность электронной подписи (в том случае, если информация о дате и времени подписания электронного документа отсутствует).

5.9.3. Обязательным приложением к заявлению на проверку подлинности электронной подписи в электронном документе является носитель, содержащий:

- сертификат, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе – в виде файла стандарта CMS;
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

5.9.4. Проведение работ по проверке подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

5.9.5. Результатом проведения работ по проверке подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра. Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- данные, предоставленные комиссии для проведения проверки;
- результат проверки электронной подписи электронного документа.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

5.9.6. Срок проведения работ по проверке подлинности электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет 10 (десять) рабочих дня с момента поступления заявления в Удостоверяющий центр и при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

5.9.7. В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по проверке подлинности электронной подписи осуществляется в рамках заключения отдельного договора между Удостоверяющим центром и Стороной, присоединившейся к Регламенту. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором.

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

5.10.1. Удостоверяющий центр предоставляет актуальную информацию о статусе сертификатов посредством сервиса Службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов формирует и предоставляет по запросам владельцев информацию о статусе проверяемого сертификата посредством протокола Online Certificate Status Protocol (OCSP). Адреса обращения к Службе актуальных статусов сертификатов:
http://ocsp.taxnet.ru/ocsp/ocsp.srf

http://ocsp.taxnet.ru/ocsp2.0/ocsp.srf
http://ocsp.taxnet.ru/ocsp2.0nq/ocsp.srf

5.10.2. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых сертификатов.

5.10.3. Удостоверяющий центр выдает штампы времени посредством сервиса Службы штампов времени. Служба штампов времени функционирует по протоколу Time Stamping Protocol (TSP). Адрес обращения к Службе штампов времени – https://tsp.taxnet.ru/tsp/tsp.srf.

6. Дополнительные положения

6.1. Конфиденциальность информации

6.1.1. Типы конфиденциальной информации:

- маркер временного доступа является конфиденциальной информацией. Удостоверяющий центр не осуществляет хранение маркеров временного доступа;
- ключ электронной подписи владельца сертификата является конфиденциальной информацией. Удостоверяющий центр не осуществляет хранение ключей электронной подписи;
- персональная и корпоративная информация о владельцах сертификатов, не подлежащая непосредственной рассылке в качестве части сертификата, считается конфиденциальной;
- информация, хранящаяся в Удостоверяющем центре, считается конфиденциальной и не подлежит разглашению.

6.1.2. Обработка персональных данных заявителей и владельце сертификатов.

Цель обработки персональных данных Удостоверяющим центром – идентификация и аутентификация субъекта персональных данных в качестве пользователя УЦ, а также пользователя информационных систем с применением электронной подписи, в которых используются сертификаты владельцев.

Сбор, систематизация, накопление, хранение, обновление, изменение, использование, распространение, блокирование, уничтожение персональных данных Удостоверяющим центром осуществляется согласно требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и в целях выполнения функций, полномочий и обязанностей, возложенных на аккредитованный Удостоверяющий центр Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

В соответствии с положениями подпункта 2 пункта 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» согласие субъекта персональных данных на обработку его персональных данных не требуется.

Персональные данные, обрабатываемые Удостоверяющим центром: фамилия, имя, отчество, паспортные данные, СНИЛС, идентификационный номер налогоплательщика, адрес электронной почты, контактный телефон, должность.

Персональные данные, включаемые в сертификаты, создаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

6.1.3. Типы информации, не являющейся конфиденциальной:

- Информация, не являющейся конфиденциальной информацией, считается открытой информацией.

- Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации также определяется решением Удостоверяющего центра.
- Информация, включаемая в сертификаты и в списки отозванных сертификатов, создаваемые Удостоверяющим центром, не считается конфиденциальной.
- Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

6.1.4. Исключительные полномочия Удостоверяющего центра:

- Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.
- Удостоверяющий центр оставляет за собой право использовать предоставленные заявителем или доверенным лицом заявителя контактные данные (номер мобильного телефона, адрес электронной почты) для отправки от своего имени сообщений технического или коммерческого характера. Владелец сертификата имеет право отписаться от рассылки в любой момент времени, воспользовавшись личным кабинетом на сайте Удостоверяющего центра или обратившись в службу поддержки клиентов.

6.2. Хранение сертификатов в Удостоверяющем центре

6.2.1. Срок хранения сертификатов в Удостоверяющем центре осуществляется в течение всего периода его действия и 5 (Пять) лет после прекращения его действия. По истечении указанного срока хранения сертификаты переводятся в режим архивного хранения.

6.2.2. Архивное хранение.

Удостоверяющий центр осуществляет архивное хранение электронных документов и документов на бумажных носителях информации в соответствии с законодательством Российской Федерации об архивах и архивном деле и нормативно-методическими документами Росархива, определяющих порядок работы электронного архива организации.

Документы, подлежащие архивному хранению, являются документами временного хранения. Сроки хранения архивных документов устанавливаются Приказом Министерства культуры и массовых коммуникаций РФ от 31.07.2007 г. № 1182 (ред. от 28.04.2011г.) «Об утверждении перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

6.2.3. Уничтожение архивных документов.

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Удостоверяющего центра и назначаемой приказом руководителя Удостоверяющего центра.

6.3. Обстоятельства непреодолимой силы (форс-мажор)

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.

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.

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

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.

Не извещение 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.

6.4. Права использования Программного Обеспечения

6.4.1. Право на использование ПО на условиях простой (неисключительной) лицензии предоставляется в момент создания Удостоверяющим центром сертификата.

6.4.2. Право на использование ПО предоставляется на срок действия сертификата и может использоваться в следующем объеме: установить ПО, записать и хранить ПО в память ЭВМ, а также осуществлять иные действия, необходимые для функционирования ПО в соответствии с его назначением.

6.5. Ответственность Сторон

6.5.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

6.5.2. 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.

6.5.3. 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 Стороны, присоединившейся к Регламенту, и в предоставленных документах.

6.5.4. Удостоверяющий центр не несёт ответственности за компрометацию или утерю маркера временного доступа и не возмещает ущерб, причиненный данными обстоятельствами Стороне, присоединившейся к Регламенту.

6.5.5. Удостоверяющий центр не несёт ответственности за компрометацию или утерю ключей электронной подписи и не возмещает ущерб, причиненный данными обстоятельствами Стороне, присоединившейся к Регламенту.

6.5.6. Удостоверяющий центр несет ответственность за убытки при использовании изготовленного Удостоверяющим центром ключа электронной подписи и сертификата в том случае, если данные убытки возникли по причине нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра.

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

6.6. Разрешение споров

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

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

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

6.6.4. Споры между сторонами, неурегулированные в процессе совместных переговоров, разрешаются в судебном порядке в соответствии с действующим законодательством Российской Федерации.

6.7. Прекращение деятельности

6.7.1. Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном законодательством Российской Федерации.

6.7.2. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан:

- сообщить об этом в уполномоченный федеральный орган не позднее, чем за один месяц до даты прекращения своей деятельности;
- передать в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в Удостоверяющем центре.

6.8. Структура сертификатов и реестра отозванных сертификатов

Удостоверяющий центр издает сертификаты в форме электронного документа формата X.509 версии 3 и ведет Реестр отозванных сертификатов в электронной форме формата X.509 версии 2.

6.8.1. Структура квалифицированного сертификата ключа проверки электронной подписи описана в Приложении № 10.

6.8.2. Структура неквалифицированного сертификата ключа проверки электронной подписи описана в Приложении № 11.

6.8.3. Формат списка отозванных сертификатов (CRL) Удостоверяющего центра:

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки события, повлекшего прекращение или приостановление действия сертификата (Time) 3. Код причины прекращения действия сертификата (Reson Code) "0" Не указана "1" Компрометация ключа (нарушение конфиденциальности ключа) "2" Компрометация ЦС (нарушение конфиденциальности ключа Удостовоеряющего центра) "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
signatureAlgorithm	Алгоритм электронной подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA Version	Объектный идентификатор сертификата издателя	Версия сертификата Удостоверяющего Центра

6.8.4. Обеспечение актуальности информации, содержащейся в Реестре сертификатов КЭП, и ее защиты.

Актуальность информации в Реестре сертификатов КЭП обеспечивается с использованием средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, которые в режиме реального времени заносят информацию в Реестр.

Защита информации, содержащейся в Реестре сертификатов КЭП, от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий обеспечивается путем размещения технических средств удостоверяющего центра в контролируемой зоне, исключающей свободное пребывание посторонних лиц, использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, систем резервного копирования и систем разграничения доступа.

6.9. Порядок ведения реестра сертификатов

6.9.1. Форматы ведения реестра сертификатов.

Ведение реестра сертификатов включает в себя:

- внесение изменений в реестр сертификатов в случае изменения сведений;
- внесение в реестр сертификатов сведений о прекращении действия или об аннулировании сертификатов.

Реестр выданных сертификатов ведется в электронной форме в формате базы данных с использованием сертифицированных средств удостоверяющего центра.

Удостоверяющий центр безвозмездно предоставляет любому лицу по его обращению доступ к информации, содержащейся в реестре сертификатов, в том числе информацию об аннулировании сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов и направляется обратившемуся лицу как почтовым отправлением, так и с использованием информационно-телекоммуникационных сетей (по выбору лица, обратившегося за получением информации из реестра сертификатов).

Срок предоставления указанной информации не превышает 7 (семи) дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно-телекоммуникационных сетей.

6.9.2. Сроки внесения информации о прекращения действия или аннулировании сертификата в реестр сертификата не превышает 12 (двенадцать) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

6.10. Порядок планового и внепланового технического обслуживания реестра сертификатов.

Удостоверяющий центр осуществляет плановое техническое обслуживание реестра сертификатов 1 раз в месяц во внерабочее время. Время проведения работ составляет не боле 1 часа.

Внеплановое техническое обслуживание проводится при появлении такой необходимости в оперативном режиме. Врем проведения работ составляет не более 1 часа.

Время проведения технического обслуживания реестра сертификатов может быть увеличено по объективным причинам.

Удостоверяющий центр информирует участников информационного взаимодействия о проведении технического обслуживания путем размещения уведомления на официальном сайте www.taxnet.ru

6.11. Порядок исполнения обязанностей Удостоверяющего центра

6.11.1. Информирование заявителей об условиях и о порядке использования электронной подписи и средств электронной подписи, о рисках, связанных с использованием электронных подписей и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, осуществляется методом индивидуального устного информирования заявителя в процессе выдачи ему сертификата КЭП, а также путем выдачи совместно с сертификатом КЭП руководства по обеспечению безопасности использования

электронной подписи и средств электронной подписи, включающего рекомендации по использованию сертифицированных ключевых носителей.

6.11.2. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности. Защита информации, содержащейся в Реестре сертификатов КЭП обеспечивается путем размещения технических средств удостоверяющего центра в контролируемой зоне, исключающей свободное пребывание посторонних лиц, использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, систем резервного копирования и систем разграничения доступа.

Хранение информации, содержащейся в реестре сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему. Для предотвращения утраты сведений о сертификатах, содержащихся в реестре, формируется его резервная копия.

6.11.3. Удостоверяющий центр обеспечивает круглосуточную доступность реестра сертификатов в информационно-коммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания реестра сертификатов, при этом Удостоверяющий центр обязан обеспечить безвозмездный доступ в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

6.11.4. Удостоверяющий центр обеспечивает конфиденциальность созданных Удостоверяющим центром ключей электронных подписей. Ключ электронной подписи, соответствующий сертификату, является конфиденциальной информацией владельца сертификата. Удостоверяющий центр не осуществляет хранение ключей электронной подписи. Созданные ключи электронной подписи незамедлительно передаются заявителю.

6.11.5. Удостоверяющий центр производит регистрацию сертификата КЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона от 06.04.2011г. № 63-ФЗ «Об Электронной подписи».

6.11.6. При выдаче сертификата КЭП, Удостоверяющий центр по желанию лица, которому выдан сертификат КЭП, безвозмездно осуществляет регистрацию указанного лица в Единой системе идентификации и аутентификации.

7. Список приложений

Приложения № 1.а-1.в. Формы заявлений о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет».

Приложение № 2.а-2.в. Формы заявлений на создание и выдачу сертификата ключа проверки электронной подписи.

Приложения № 3.а-3.б. Формы Доверенностей (на осуществление действий в рамках Регламента УЦ ЗАО «ТаксНет»).

Приложения № 4.а-4.в. Формы Доверенностей (на получение ключей электронной подписи и сертификата ключа проверки электронной подписи).

Приложения № 5.а-5.в. Формы заявлений на аннулирование сертификата ключа проверки электронной подписи.

Приложения № 6.а-6.в. Формы заявлений на приостановление действия сертификата ключа проверки электронной подписи.

Приложение № 7.а-7.в. Формы заявлений на возобновление действия сертификата ключа проверки электронной подписи.

Приложение № 8.а-8.в. Формы заявлений на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ЗАО «ТаксНет».

Приложения № 9.а-9.в. Формы заявлений для проверки подлинности электронной подписи в электронных документах.

Приложение № 10. Структура квалифицированного сертификата ключа проверки электронной подписи.

Приложение № 11. Структура неквалифицированного сертификата ключа электронной подписи.

Приложение № 1.а
(Форма для юридических лиц)

Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет»[1]

_____
(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____
(основание)

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра ЗАО «ТаксНет», условия которого определены ЗАО «ТаксНет» и опубликованы на сайте Удостоверяющего центра ЗАО «ТаксНет» по адресу http://taxnet.ru/download/uc_reglament.pdf

С Регламентом Удостоверяющего центра ЗАО «ТаксНет» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Руководитель организации _____/_____
(подпись) (ФИО)

«____» _____20___год
(дата подписания заявления)

М.П.

(заполняется Удостоверяющим центром)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет» зарегистрировано в реестре Удостоверяющего центра. Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо
Удостоверяющего центра
ЗАО «ТаксНет» _____/_____
(подпись) (ФИО)

М.П.

[1] Заявление о присоединении к Регламенту подается в Удостоверяющий центр в **двух** экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю.

Приложение № 1.б
(Форма для индивидуальных предпринимателей)

Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет»[1]

_____
(полное наименование ИП)

действующий на основании _____
(основание)

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра ЗАО «ТаксНет», условия которого определены ЗАО «ТаксНет» и опубликованы на сайте Удостоверяющего центра ЗАО «ТаксНет» по адресу http://taxnet.ru/download/uc_reglament.pdf

С Регламентом Удостоверяющего центра ЗАО «ТаксНет» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

_____/_____
(подпись) (ФИО)

«____» _____20___год
(дата подписания заявления)

М.П.

(заполняется Удостоверяющим центром)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет» зарегистрировано в реестре Удостоверяющего центра. Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо
Удостоверяющего центра
ЗАО «ТаксНет» _____/_____
(подпись) (ФИО)

М.П.

[1] Заявление о присоединении к Регламенту подается в Удостоверяющий центр в **двух** экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю.

Приложение № 1.в
(Форма для физических лиц)

Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет»[1]

Я, _____
(ФИО)

серия _____ номер _____
(серия и номер паспорта)

выдан _____
(кем и когда выдан)

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра ЗАО «ТаксНет», условия которого определены ЗАО «ТаксНет» и опубликованы на сайте Удостоверяющего центра ЗАО «ТаксНет» по адресу http://taxnet.ru/download/uc_reglament.pdf

С Регламентом Удостоверяющего центра ЗАО «ТаксНет» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

_____/_____
(подпись) (ФИО)

«____» _____20___год
(дата подписания заявления)

(заполняется Удостоверяющим центром)

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «ТаксНет» зарегистрировано в реестре Удостоверяющего центра. Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо
Удостоверяющего центра
ЗАО «ТаксНет» _____/_____
(подпись) (ФИО)

М.П.

[1] Заявление о присоединении к Регламенту подается в Удостоверяющий центр в **двух** экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю.

Приложение №2.а
(Форма для юридических лиц)

Заявление на создание и выдачу сертификата ключа проверки электронной подписи

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

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

действующего на основании _____
(основание полномочий)

просит создать сертификат ключа проверки электронной подписи уполномоченного представителя

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными[1]:

Фамилия, Имя, Отчество	
Адрес электронной почты	
Должность/Звание	
Наименование подразделения	
Краткое наименование организации	
Адрес места нахождения организации	
ОГРН	
СНИЛС владельца сертификата	
ИНН организации	
Город	
Область	
Страна	RU
Тип сертификата	

Владелец сертификата ключа проверки ЭП _____/_____/

«____» _____ 201__ г.

Руководитель организации _____/_____/

«____» _____ 201__ г.

М.П.

---

*Сведения в заявлении сверены с реквизитами СНИЛС и документа, удостоверяющего личность заявителя.

Сверил(а) _____(_____)
(подпись) (ФИО)

«____»_____201__г.

[1] Обработка персональных данных Удостоверяющим центром ЗАО «ТаксНет» осуществляется согласно требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и в целях выполнения функций, полномочий и обязанностей, возложенных на аккредитованный удостоверяющий центр Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». В соответствии с положениями подпункта 2 пункта 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» согласие субъекта персональных данных на обработку его персональных данных не требуется.

Приложение №2.б
(Форма для индивидуальных предпринимателей)

Заявление на создание и выдачу сертификата ключа проверки электронной подписи

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

просит создать сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными[1]:

Фамилия, Имя, Отчество	
Адрес электронной почты	
Адрес места регистрации	
ОГРНИП	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU
Тип сертификата	

Владелец сертификата ключа проверки ЭП _____/_____/

«____» _____ 201__ г.

М.П.

_____

*Сведения в заявлении сверены с реквизитами СНИЛС и документа, удостоверяющего личность заявителя.

Сверил(а) _____(_____)
(подпись) (ФИО)

«____»_____201__г.

[1] Обработка персональных данных Удостоверяющим центром ЗАО «ТаксНет» осуществляется согласно требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональ[1]ных данных» и в целях выполнения функций, полномочий и обязанностей, возложенных на аккредитованный удостоверяющий центр Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». В соответствии с положениями подпункта 2 пункта 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» согласие субъекта персональных данных на обработку его персональных данных не требуется.

Приложение №2.в
(Форма для физических лиц)

Заявление на создание и выдачу сертификата ключа проверки электронной подписи

Я, _____
(ФИО)

серия _____ номер _____
(серия и номер паспорта, кем и когда выдан)

прошу создать сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении моими идентификационными данными[1]:

Фамилия, Имя, Отчество	
Адрес электронной почты	
Адрес места регистрации	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU
Тип сертификата	

_____/_____/
(подпись) (ФИО)

«____» _____ 201__ г.

*Сведения в заявлении сверены с реквизитами СНИЛС и документа, удостоверяющего личность заявителя.

Сверил(а) _____/_____/
(подпись) (ФИО)

«____» _____ 201__ г.

[1] Обработка персональных данных Удостоверяющим центром ЗАО «ТаксНет» осуществляется согласно требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональ[1] ных данных» и в целях выполнения функций, полномочий и обязанностей, возложенных на аккредитованный удостоверяющий центр Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». В соответствии с положениями подпункта 2 пункта 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» согласие субъекта персональных данных на обработку его персональных данных не требуется.

Приложение № 3.а
(Форма для юридических лиц)

Доверенность № _____

Дата выдачи: "_____"_____ 201__ года

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

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

действующего на основании _____
(основание полномочий)

в соответствии со Ст. 185 Гражданского кодекса Российской Федерации уполномочивает представителя своей организации _____
(фамилия, имя, отчество уполномоченного представителя)

_____
(серия и номер паспорта, кем и когда выдан)

действовать от имени _____
(наименование организации)

при использовании электронной подписи и осуществлять действия в рамках Регламента Удостоверяющего центра ЗАО «ТаксНет», установленные для владельца сертификата, в том числе получить ключи электронной подписи и сертификат ключа проверки электронной подписи.
Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

Настоящая доверенность действительна по «____» _____ 201___ г.
(не более 1 года)

Подпись уполномоченного представителя _____/_____ подтверждаю.
(подпись) (ФИО)

Руководитель организации _____/ _____
(подпись) (ФИО)

«___»_____201__г.
(дата подписания)

М.П.

---

*Сведения в доверенности сверены с реквизитами документа, удостоверяющего личность заявителя.

Сверил(а) _____(_____)
(подпись) (ФИО)

«____»_____201__г.

Приложение № 3.б
(Форма для индивидуальных предпринимателей)

Доверенность № _____

Дата выдачи: "_____"_____ 201__ года

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

в соответствии со Ст. 185 Гражданского кодекса Российской Федерации уполномочивает _____

_____
(фамилия, имя, отчество уполномоченного представителя)

_____
(серия и номер паспорта, кем и когда выдан)

действовать от имени _____
(наименование ИП)

при использовании электронной подписи и осуществлять действия в рамках Регламента Удостоверяющего центра ЗАО «ТаксНет», установленные для владельца сертификата, в том числе получить ключи электронной подписи и сертификат ключа проверки электронной подписи.
Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

Настоящая доверенность действительна по «____» _____ 201___ г.
(не более 1 года)

Подпись уполномоченного представителя_____/_____ подтверждаю.
(подпись) (ФИО)

Индивидуальный предприниматель _____/ _____
(подпись) (ФИО)

«___»_____201__г.
(дата подписания)

М.П.

---

*Сведения в доверенности сверены с реквизитами документа, удостоверяющего личность получателя.

Сверил(а) _____(_____)
(подпись) (ФИО)

«____»_____201__г.

Приложение №4.а
(Форма для юридических лиц)

Доверенность № _____

Дата выдачи: "_____" _____ 201__ года

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

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

действующего на основании _____
(основание полномочий)

в соответствии со Ст.18 Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи» и Ст. 185 Гражданского кодекса Российской Федерации уполномочивает представителя своей организации

_____
(фамилия, имя, отчество уполномоченного представителя)

_____
(серия и номер паспорта, кем и когда выдан)

1. предоставить в Удостоверяющий центр ЗАО «ТаксНет» необходимые документы, определенные Регламентом Удостоверяющего центра ЗАО «ТаксНет» для создания ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи

_____
(фамилия, имя, отчество владельца сертификата)

2. получить ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, созданные для владельца сертификата и иные документы, определенные Регламентом Удостоверяющего центра ЗАО «ТаксНет».

Настоящая доверенность действительна по «____» _____ 201___ г.
(не более 10 дней)

Подпись уполномоченного представителя_____/_____ подтверждаю.
(подпись) (ФИО)

Руководитель организации _____/ _____
(подпись) (ФИО)

«___»_____201__г.
(дата подписания)

М.П.

---

*Сведения в доверенности сверены с реквизитами документа, удостоверяющего личность получателя.

Сверил(а) _____(_____)
(подпись) (ФИО)

«____»_____201__г.

Приложение №4.б
(Форма для индивидуальных предпринимателей)

Доверенность № _____

Дата выдачи: "_____" _____ 201__ года

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

в соответствии со Ст.18 Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи» и Ст. 185 Гражданского кодекса Российской Федерации уполномочивает

_____
(фамилия, имя, отчество уполномоченного представителя)

_____
(серия и номер паспорта, кем и когда выдан)

1. предоставить в Удостоверяющий центр ЗАО «ТаксНет» необходимые документы, определенные Регламентом Удостоверяющего центра ЗАО «ТаксНет» для создания ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи

_____
(фамилия, имя, отчество владельца сертификата)

2. получить ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, созданные для владельца сертификата и иные документы, определенные Регламентом Удостоверяющего центра ЗАО «ТаксНет».

Настоящая доверенность действительна по «____» _____ 201___ г.
(не более 10 дней)

Подпись уполномоченного представителя_____/_____ подтверждаю.
(подпись) (ФИО)

Индивидуальный предприниматель _____/ _____
(подпись) (ФИО)

«___»_____201__г.
(дата подписания)

М.П.

---

*Сведения в доверенности сверены с реквизитами документа, удостоверяющего личность получателя.

Сверил(а) _____(_____)
(подпись) (ФИО)

«____»_____201__г.

Приложение №4.в
(Форма для физических лиц)

Доверенность*

город_____ «_____» _____201___ г.

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

уполномочиваю _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

1. предоставить в Удостоверяющий центр ЗАО «ТаксНет» необходимые документы, определенные Регламентом Удостоверяющего центра ЗАО «ТаксНет» для создания ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на мое имя.
2. получить ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, созданные на мое имя, и иные документы, определенные Регламентом Удостоверяющего центра ЗАО «ТаксНет».

Настоящая доверенность действительна по «____» _____ 201____ г.
(не более 10 рабочих дней)

Подпись уполномоченного представителя_____/_____ подтверждаю.
(подпись) (ФИО)

«____»_____20__г. _____/_____
(подпись) (ФИО)

*Настоящая Доверенность должна быть заверена нотариусом

Приложение №5.а
(Форма для юридических лиц)

Заявление на аннулирование сертификата ключа проверки электронной подписи

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

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

действующего на основании _____
(основание полномочий)

в связи _____
(причина аннулирования сертификата)

просит аннулировать сертификат ключа проверки электронной подписи уполномоченного представителя

_____
(фамилия, имя, отчество)

содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Должность/звание	
Наименование подразделения	
Краткое наименование организации	
Адрес места нахождения организации	
ОГРН	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Владелец сертификата ключа проверки ЭП _____/_____/

«____» _____ 201__ г.

Руководитель организации _____/_____/

«____» _____ 201__ г.

М.П.

Приложение №5.б
(Форма для индивидуальных предпринимателей)

Заявление на аннулирование сертификата ключа проверки электронной подписи

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

в связи _____
(причина аннулирования сертификата)

просит аннулировать сертификат ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Адрес места регистрации	
ОГРНИП	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Индивидуальный предприниматель _____/_____/

«____» _____ 201__ г.
М.П.

Приложение №5.в
(Форма для физических лиц)

Заявление на аннулирование сертификата ключа проверки электронной подписи Пользователя УЦ ЗАО «ТаксНет»

Я, _____
(ФИО)

серия _____ номер _____
(серия и номер паспорта, кем и когда выдан)

в связи _____
(причина аннулирования сертификата)

прошу аннулировать сертификат ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Адрес места регистрации	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

«____»_____20__г. _____/_____
(подпись) (ФИО)

Приложение №6.а
(Форма для юридических лиц)

Заявление на приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ ЗАО «ТаксНет»

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

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

действующего на основании _____
(основание полномочий)

в связи _____
(причина приостановления действия сертификата)

просит приостановить действие сертификата ключа проверки электронной подписи уполномоченного представителя

_____
(фамилия, имя, отчество)

содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Должность/звание	
Наименование подразделения	
Краткое наименование организации	
Адрес места нахождения организации	
ОГРН	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Срок приостановления действия сертификата ключа проверки электронной подписи _____ дней.
(количество дней прописью)

Владелец сертификата ключа проверки ЭП _____/_____/

«____» _____ 201__ г.

Руководитель организации _____/_____/

«____» _____ 201__ г.

М.П.

Приложение №6.б
(Форма для индивидуальных предпринимателей)

Заявление на приостановление действия сертификата ключа проверки электронной подписи

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

в связи _____
(причина приостановления действия сертификата)

просит приостановить действие сертификата ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Адрес места регистрации	
ОГРНИП	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Срок приостановления действия сертификата ключа проверки электронной подписи _____ дней.
(количество дней прописью)

Индивидуальный предприниматель _____/_____/

«____» _____ 201__ г.
М.П.

Приложение №6.в
(Форма для физических лиц)

Заявление на приостановление действия сертификата ключа проверки электронной подписи

Я, _____
(ФИО)

серия _____ номер _____
(серия и номер паспорта, кем и когда выдан)

в связи _____
(причина приостановления действия сертификата)

прошу приостановить действие сертификата ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Адрес места регистрации	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Срок приостановления действия сертификата ключа проверки электронной подписи _____ дней.
(количество дней прописью)

«____»_____20__г. _____/_____
(подпись) (ФИО)

Приложение №7.а
(Форма для юридических лиц)

Заявление на возобновление действия сертификата ключа проверки электронной подписи

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

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

действующего на основании _____
(основание полномочий)

просит возобновить действие сертификата ключа проверки электронной подписи уполномоченного представителя

_____
(фамилия, имя, отчество)

содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Должность/звание	
Наименование подразделения	
Краткое наименование организации	
Адрес места нахождения организации	
ОГРН	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Владелец сертификата ключа проверки ЭП _____/_____/

«____» _____ 201__ г.

Руководитель организации _____/_____/

«____» _____ 201__ г.

М.П.

Приложение №7.а
(Форма для индивидуальных предпринимателей)

Заявление на возобновление действия сертификата ключа проверки электронной подписи

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

просит возобновить действие сертификата ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Адрес места регистрации	
ОГРНИП	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

Индивидуальный предприниматель _____/_____/

«____» _____ 201__ г.

М.П.

Приложение №7.б
(Форма для физических лиц)

Заявление на возобновление действия сертификата ключа проверки электронной подписи

Я, _____
(ФИО)

серия _____ номер _____
(серия и номер паспорта, кем и когда выдан)

прошу возобновить действие сертификата ключа проверки электронной подписи, содержащий следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Адрес электронной почты	
Адрес места регистрации	
СНИЛС	
ИНН	
Город	
Область	
Страна	RU

«____»_____20__г. _____/_____
(подпись) (ФИО)

Приложение №8.а
(Форма для юридических лиц)

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ЗАО «ТаксНет»

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

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

действующего на основании _____
(основание полномочий)

просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ЗАО «ТаксНет» и содержащего следующие данные:

Серийный номер	
Фамилия Имя Отчество	
Краткое наименование организации	

Время[7] (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Руководитель организации _____/_____/

«_____» _____ 201__г.

М.П.

[7] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром.

Приложение №8.б
(Форма для индивидуальных предпринимателей)

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ЗАО «ТаксНет»

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ЗАО «ТаксНет» и содержащего следующие данные:

Серийный номер	
Фамилия Имя Отчество	

Время[8] (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Индивидуальный предприниматель _____/_____/

«____» _____ 201__ г.

М.П.

[8] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром.

Приложение №8.б
(Форма для физических лиц)

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ЗАО «ТаксНет»

Я, _____
(фамилия, имя, отчество)

прошу предоставить информацию о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ЗАО «ТаксНет» и содержащего следующие данные:

Серийный номер	
Фамилия Имя Отчество	

Время[9] (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

«____»_____20__г. _____/_____
(подпись) (ФИО)

[9] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром.

Приложение №9.а
(Форма для юридических лиц)

Заявление на проверку подлинности электронной подписи в электронном документе

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

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

действующего на основании _____
(основание полномочий)

просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–ХХХ;

2. файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–ХХХ;

3. время[10] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»;
час минута день месяц год

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

«_____:_____» «_____/_____/_____»;
час минута день месяц год

Руководитель организации _____/_____/

«____» _____ 201__ г.
М.П.

[10] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени).

Приложение №9.б
(Форма для индивидуальных предпринимателей)

Заявление на проверку подлинности электронной подписи в электронном документе

_____
(полное наименование ИП)

действующий на основании _____
(наименование документа)

просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–XXX;

2. файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–XXX;

3. время[11] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»;
час минута день месяц год

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

«_____:_____» «_____/_____/_____»;
час минута день месяц год

Индивидуальный предприниматель _____/_____/

«____» _____ 201__ г.
М.П.

[11] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени).

Приложение №9.в
(Форма для физических лиц)

Заявление на проверку подлинности электронной подписи в электронном документе

Я, _____
(фамилия, имя, отчество)

прошу проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–XXX;

2. файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–XXX;

3. время[12] подписания электронной подписью электронного документа:
«_____:_____» «_____/_____/_____»;
час минута день месяц год

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

«_____:_____» «_____/_____/_____»;
час минута день месяц год

«____»_____20__г. _____/_____
(подпись) (ФИО)

[12] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени).

Приложение № 10

Структура квалифицированного сертификата ключа проверки электронной подписи

1. Общие сведения

Создание и выдача квалифицированного сертификата осуществляется аккредитованным Удостоверяющим центром в соответствии со ст.17 и 18 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об Электронной подписи».

Требования к форме квалифицированного сертификата, к средствам электронной подписи и средствам удостоверяющего центра устанавливаются Федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России). Форма квалифицированного сертификата, создаваемого аккредитованным Удостоверяющим центром, соответствует требованиям Приказа ФСБ России от 27 декабря 2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Владельцем квалифицированного сертификата может быть юридическое лицо, индивидуальный предприниматель и физическое лицо. В случае выдачи сертификата юридическому лицу в качестве владельца сертификата наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Допускается не указывать в качестве владельца сертификата физическое лицо, действующее от имени юридического лица, если сертификат будет применяться для автоматического создания и (или) автоматической проверки электронных подписей в отдельных информационных системах при оказании государственных и муниципальных услуг.

2. Структура квалифицированного сертификата

Таблица 1. Структура квалифицированного сертификата.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	Номер версии формата сертификата (V3)
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer	УЦ -издатель сертификата	Идентифицирует аккредитованный УЦ, доверенное лицо аккредитованного УЦ либо уполномоченный федеральный орган, создавшие и выдавшие данный сертификат.
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по (notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	SN = Фамилия владельца сертификата G = Имя и отчество (если имеется) владельца сертификата T = Должность - для юридических лиц

		UnsructuredName (UN) = INN=ИНН/KPP=КПП/OGRN=ОГРН – опционально, для индивидуальных предпринимателей; STREET = адреса места нахождения соответствующего лица, включает наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется). CN= имя, фамилию и отчество (если имеется) - для физического лица, или наименование - для юридического лица O = наименование юридического лица L = Город S = Субъект федерации C = Страна/Регион = RU E = электронная почта ИНН = ИНН владельца квалифицированного сертификата. Для юридического лица – ИНН юридического лица. Для индивидуального предпринимателя и физического лица – ИНН физического лица. ОГРН = ОГРН владельца квалифицированного сертификата - юридического лица СНИЛС = СНИЛС владельца квалифицированного сертификата - физического лица ОГРНИП = ОГРНИП владельца квалифицированного сертификата – индивидуального предпринимателя
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer Signature	ЭП УЦ - издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Authority Key Identifier	Идентификатор ключа УЦ - издателя сертификата	Идентификатор ключа подписи Удостоверяющего центра, на котором подписан данный сертификат.
Key Usage (critical)	Область использования ключа	Информация об использовании ключа. Значение данного поля должно обеспечивать использование ключа для формирования ЭП и шифрования данных
Certificate Policies	Политика сертификации	[1] Политика сертификата Идентификатор политики=Класс средства ЭП КС1 [2] Политика сертификата Идентификатор политики=Класс средства ЭП КС2
Subject Sign Tool	Средство ЭП владельца сертификата	Наименование средства ЭП владельца сертификата.
Issuer Sign Tool	Средство ЭП и средство УЦ, использующиеся для создания сертификатов	Наименование средства ЭП и средства УЦ, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством РФ.
SubjectKeyIdendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа подписи владельца сертификата
ExtendedKeyUsage (необязательное дополнение)	Расширенная область использования ключа	Набор расширенных областей использования ключа-объектных идентификаторов.
CRL Distribution Point (необязательное дополнение)	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов.
Authority Information Access (необязательноедополнение)	Адрес Службы актуальных статусов сертификатов, Адрес размещения информации о сертификате УЦ	URLадреса Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP: URL=http://ocsp.taxnet.ru/ocsp/ocsp.srf URL=http://ocsp.taxnet.ru/ocsp2.0/ocsp.srf
Private Key Period (необязательное дополнение)	Период использования ключа подписи	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC

В сертификат могут быть добавлены дополнительные поля и дополнения согласно RFC 5280.

3. Сведения о владельце сертификата

Владелец сертификата идентифицируется по данным, содержащимся в поле «Subject».

Таблица 2. Таблица заполнения поля «Subject» квалифицированного сертификата.

	Физическое лицо (ФЛ)	Физическое лицо – индивидуальный предприниматель (ИП)	Российское юридическое лицо (ЮЛ)	Автоматическое создание и/или проверка ЭП (российское юридическое лицо)	Иностранное юридическое лицо	Автоматическое создание и/или проверка ЭП (иностранное юридическое лицо)
CommonName (общее имя)	ФИО ФЛ	ФИО ФЛ	Наименование организации	Наименование организации	Наименование организации	Наименование организации
Surname (фамилия)	Фамилия ФЛ	Фамилия ФЛ	Фамилия представителя ЮЛ	-	Фамилия представителя	-
GivenName (имя и отчество, (если имеется))	Имя и отчество ФЛ	Имя и отчество ФЛ	Имя и отчество представителя ЮЛ	-	Имя и отчество представителя ЮЛ	-
CountryName (наименование страны) - двухсимвольный код страны	+	+	+	+	+	+
StateOrProvinceName (наименование области)	+	+	+	+	-	-
LocalityName (наименование населенного пункта)	+	+	+	+	+	+
StreetAddress (название улицы, номер дома)	+	+	+	+	+	+
OrganizationName (наименование организации)	-	-	+	+	+	+
OrganizationUnitName (подразделение)	-	-	+	опционально	+	опционально
Title (должность представителя)	-	-	+	-	+	-
E-mail (адрес электронной почты)	+	+	+	+	+	+
OGRN (ОГРН)	-	-	+	+	-	-
SNILS (СНИЛС)	+	+	СНИЛС представителя ЮЛ	-	-	-
INN (ИНН)	+	+	ИНН ЮЛ	ИНН ЮЛ	ИНН ЮЛ	ИНН ЮЛ
OGRNIP (ОГРНИП)	-	+	-	-	-	-

4. Сведения об областях применения квалифицированного сертификата

Таблица 3. Список объектных идентификаторов квалифицированного сертификата.

ОИД	Описание
Базовые ОИДы поля Extended Key Usage	
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента
1.3.6.1.5.5.7.3.4	Защищенная электронная почта
1.2.643.2.2.34.6	Пользователь Центра Регистрации, HTTP, TLS клиент
Дополнительные ОИДы поля Extended Key Usage	
1.2.643.100.2.1	Доступ к СМЭВ ЭП-СП
1.2.643.100.2.2	Доступ к СМЭВ ЭП-ОВ
1.2.643.3.215.11	Уполномоченные лица - работники организации - уполномоченного экономического оператора
1.2.643.3.215.12	Лица, с которыми ФТС России заключен соответствующий договор поручительства
1.2.643.3.215.13	Резидент ОЭЗ (нерезидент ОЭЗ) или лицо, действующее по его поручению на основании доверенности
1.2.643.3.215.4	Перевозчики, таможенные представители от имени перевозчика либо иные лица, действующие по поручению перевозчика
1.2.643.3.215.6	Перевозчики, иные лица, обладающие полномочиями в отношении товаров, или их представители
1.2.643.3.215.7	Владелец СВХ (лицо, осуществляющее временное хранение товаров в ином месте временного хранения). Руководитель организации, главный бухгалтер либо лицо, ими уполномоченное
1.2.643.3.215.8	Уполномоченные лица организации - таможенного представителя
1.2.643.3.241	Использование в работе систем ЗАО ТЭК-Торг
1.2.643.3.8.100.1.42	Использование ЭП на ЭТП Объединенная торговая площадка
1.2.643.5.1.24.2.1.3	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости - Правообладатель Физическое лицо или его законный представитель; лицо, получившее доверенность от правообладателя или его законного представителя
1.2.643.5.1.24.2.1.3.1	Формирование кадастровым инженером документов как результат кадастровых работ - Кадастровый инженер
1.2.643.5.1.24.2.19	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости - Руководитель органа местного самоуправления или иное уполномоченное лицо данного органа в соответствии с федеральным законом
1.2.643.5.1.24.2.27	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним - Арбитражный управляющий
1.2.643.5.1.24.2.30	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости - Правообладатель Юридическое лицо

1.2.643.5.1.24.2.49	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним и о предоставлении сведений из государственного кадастра недвижимости - Руководители (заместители руководителей) многофункциональных центров предоставления государственных и муниципальных услуг
1.2.643.5.1.28.2	Система декларирования ФСРАР
1.2.643.5.1.28.3	Система декларирования ФСРАР-розничная АП
1.2.643.5.1.28.4	Система декларирования ФСРАР-лицензиат
1.2.643.6.14	Использование в работе систем ООО Центр Реализации
1.2.643.6.15	Использование в работе систем ЭТП Фабрикант
1.2.643.6.17.1	Использование в работе систем ЭТП ГПБ
1.2.643.6.18.1	Организатор торгов на ЭТП ЦДТ
1.2.643.6.18.2	Участник торгов на ЭТП ЦДТ
1.2.643.6.3	Использование в электронных торговых системах и в программном обеспечении, связанном с обменом электронными сообщениями
1.2.643.6.3.1.1	Использование на электронных площадках, отобранных для проведения аукционов в электронной форме
1.2.643.6.3.1.2.1	Участник торгов - Юридическое лицо
1.2.643.6.3.1.2.2	Участник торгов - Физическое лицо
1.2.643.6.3.1.2.3	Участник торгов - Индивидуальный предприниматель
1.2.643.6.3.1.3.1	Участник размещения заказа
1.2.643.6.3.1.4.1	Полномочия участника торгов - Администратор организации
1.2.643.6.3.1.4.2	Полномочия участника торгов - Уполномоченный специалист
1.2.643.6.3.1.4.3	Полномочия участника торгов - Специалист с правом подписи контракта
1.2.643.6.3.2	Использование в информационной системе по раскрытию существенных фактов деятельности юридических лиц
1.2.643.6.37.1.1	Система электронных паспортов транспортных средств
1.2.643.6.40.1	Участник, имеющий право на раскрытие информации, АО «СКРИН»
1.2.643.6.41.1.1.1	Участник, имеющий право на раскрытие информации, ООО «Интерфакс-ЦРКИ»
1.2.643.6.42.5.5.5	Участник, имеющий право на раскрытие информации, ЗАО «АЭИ «Прайм»
1.2.643.6.44.1.1.1	Участник, имеющий право на раскрытие информации, АНО «АЗИПИ»
1.2.643.6.45.1.1.1	Участник, имеющий право на раскрытие информации, ЗАО «АКиМ»
1.2.643.6.7	Использование в работе систем электронного документооборота и электронных систем B2B-Center
1.3.6.1.4.1.24138.1.1.2.4	Использование в работе систем Федеральных ЭТП (Combo, 12 месяцев)
1.3.6.1.4.1.24138.1.1.2.5	Использование в работе систем Коммерческих ЭТП (Combo, 12 месяцев)
1.3.6.1.4.1.24138.1.1.2.6	Использование в работе систем Федеральных ЭТП (Combo, 15 месяцев)
1.3.6.1.4.1.24138.1.1.2.7	Использование в работе систем Коммерческих ЭТП (Combo, 15 месяцев)
1.3.6.1.4.1.24138.1.1.3.1	Пользователь системы электронного документооборота с органами государственной исполнительной власти

1.3.6.1.4.1.24138.1.1.3.2	Орган государственной исполнительной власти
1.3.6.1.4.1.24138.1.1.3.3	Специализированный оператор связи системы электронного документооборота с органами государственной исполнительной власти
1.3.6.1.4.1.24138.1.1.3.6	Регистрация сертификата в системе «Альта-софт»
1.3.6.1.4.1.24138.1.1.3.7	Регистрация кассового аппарата ККМ
1.3.6.1.4.1.24138.1.1.3.8	Пользователь программы "Криптекс"
1.3.6.1.4.1.24138.1.1.4.3	Стандартный (для ЮЛ, срок действия 12 месяцев)
1.3.6.1.4.1.24138.1.1.4.4	Стандартный (для ИП, срок действия 12 месяцев)
1.3.6.1.4.1.24138.1.1.6.1	Системы электронного документооборота муниципальных образований
1.3.6.1.4.1.24138.1.1.8.1	Обеспечение юридической значимости в электронных торговых системах
1.3.6.1.4.1.24138.1.1.8.3	Стандартный Портал
1.3.6.1.4.1.24138.1.1.8.4	Стандартный (для ФЛ, срок действия 3 месяца)
1.3.6.1.4.1.24138.1.1.8.5	Стандартный (для ФЛ, срок действия 12 месяцев)
1.3.6.1.4.1.24138.1.1.8.6	Подписание документов в рамках информационных систем органов государственной власти
1.3.6.1.4.1.24138.1.1.8.7	Для использования в государственных информационных системах
1.3.6.1.4.1.24138.1.1.8.8	Использование на электронных площадках, отобранных для проведения аукционов в электронной форме (3 месяца)
1.3.6.1.4.1.24138.1.1.9.1	Информационное взаимодействие с контролирующими органами

Приложение № 11

Структура неквалифицированного сертификата ключа проверки электронной подписи

1. Общие сведения

Создание и выдача неквалифицированного сертификата осуществляется аккредитованным Удостоверяющим центром в соответствии со ст.14 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об Электронной подписи» и положениями Регламента получения сертификатов ключей подписей и использования электронной цифровой подписи от 09.08.2010 г.
Фактом заключения соглашения об использовании НЭП является присоединение заявителя к Регламенту Удостоверяющего центра ЗАО «ТаксНет».

2. Структура неквалифицированного сертификата.

Таблица 1. Структура неквалифицированного сертификата.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	Номер версии формата сертификата (V3)
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	Идентифицирует аккредитованный УЦ, доверенное лицо аккредитованного УЦ либо уполномоченный федеральный орган, создавшие и выдавшие данный сертификат
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	SN = Фамилия владельца сертификата; G = Имя и отчество (если имеется) владельца сертификата; T = Должность - для юридических лиц; UnsructuredName (UN) = INN=ИНН/KPP=КПП/OGRN=ОГРН - для юридических лиц; STREET = адреса места нахождения соответствующего лица, включает наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется) CN = ФИО владельца сертификата OU = Подразделение - для юридических лиц O = Наименование организации - для юридических лиц; L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта ИНН = ИНН владельца квалифицированного сертификата-юридического лица ОГРН = ОГРН владельца квалифицированного сертификата - юридического лица СНИЛС = СНИЛС владельца квалифицированного сертификата - физического лица В поле Subject сертификата могут быть добавлены дополнительные компоненты имени, согласно RFC 5280
Public Key	Ключ проверки	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Информация об использовании ключа. Значение данного поля должно обеспечивать использование ключа для формирования ЭП и шифрования данных
Extended Key Usage	Улучшеный ключ	Указываются идентификаторы областей использования ключей электронных подписей и сертификатов ключей электронных подписей: Проверка подлинности клиента (OID 1.3.6.1.5.5.7.3.2) Защищенная электронная почта (OID 1.3.6.1.5.5.7.3.4)
Certificate Policies	Политика сертификации	[1] Политика сертификата Идентификатор политики=Класс средства ЭП КС1 [2] Политика сертификата

		Идентификатор политики=Класс средства ЭП КС2
Subject Sign Tool	Средство ЭП владельца сертификата	Наименование средства ЭП владельца сертификата.
Issuer Sign Tool	Средство ЭП и средство УЦ, использующиеся для создания сертификатов	Наименование средства ЭП и средства УЦ, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством РФ.
Application Policy	Политика применения	Использование на электронных площадок отобранных для проведения аукционах в электронной форме (OID 1.2.643.6.3.1.1) Области использования согласно заявлению на создание и выдачу сертификата: i. Тип участника (один вариант из списка) 1. Юридическое лицо(OID 1.2.643.6.3.1.2.1) 2. Физическое лицо(OID 1.2.643.6.3.1.2.2) 3. Индивидуальный предприниматель(OID 1.2.643.6.3.1.2.3) ii. Тип организации: 1. Участник размещения заказа(OID 1.2.643.6.3.1.3.1)
Certificate Policies	Политики сертификатов	Набор дополнительных областей использования ключей и сертификатов
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа электронной подписи владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа электронной подписи Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков аннулированных сертификатов следующего вида: URL=http://ResourceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка аннулированных сертификатов, Name - имя файла списка аннулированных сертификатов.
Authority Information Access (необязательноедополнение)	Адрес Службы актуальных статусов сертификатов, Адрес размещения информации о сертификате УЦ	URLадреса Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP: URL=http://ocsp.taxnet.ru/ocsp2.0nq/ocsp.srf

3. Сведения о владельце сертификата

Владелец сертификата идентифицируется по данным, содержащимся в поле «Subject».

Таблица 2. Таблица заполнения поля «Subject» неквалифицированного сертификата.

	Российское юридическое лицо (ЮЛ)	Иностранное юридическое лицо
CommonName (общее имя)	ФИО представителя ЮЛ	ФИО представителя ЮЛ
Title (должность представителя)	+	+
OrganizationName (наименование организации)	+	+
OrganizationUnitName (подразделение) - опционально	+	+
LocalityName (наименование населенного пункта)	+	+
StateOrProvinceName (наименование области)	+	-
CountryName (наименование страны) - двухсимвольный код страны	+	+
E-mail (адрес электронной почты)	+	+
StreetAddress (название улицы, номер дома) - опционально	+	+
SNILS (СНИЛС) - опционально	СНИЛС представителя ЮЛ	-
INN (ИНН)	ИНН ЮЛ	ИНН ЮЛ
OGRN (ОГРН)	+	-
КПП	+	-

4. Сведения об областях применения неквалифицированного сертификата

Таблица 3. Список объектных идентификаторов квалифицированного сертификата.

ОИД	Описание
Базовые ОИДы поля Extended Key Usage	
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента
1.3.6.1.5.5.7.3.4	Защищенная электронная почта
1.2.643.2.2.34.6	Пользователь Центра Регистрации, HTTP, TLS клиент
Дополнительные ОИДы поля Extended Key Usage	

1.2.643.6.3	Использование в электронных торговых системах и в программном обеспечении, связанном с обменом электронными сообщениями
1.2.643.6.3.1.1	Использование на электронных площадках, отобранных для проведения аукционов в электронной форме
1.2.643.6.3.1.2.1	Участник торгов - Юридическое лицо
1.2.643.6.3.1.2.2	Участник торгов - Физическое лицо
1.2.643.6.3.1.2.3	Участник торгов - Индивидуальный предприниматель
1.2.643.6.3.1.3.1	Участник размещения заказа
1.2.643.6.3.1.4.1	Полномочия участника торгов - Администратор организации
1.2.643.6.3.1.4.2	Полномочия участника торгов - Уполномоченный специалист
1.2.643.6.3.1.4.3	Полномочия участника торгов - Специалист с правом подписи контракта
1.2.643.6.7	Использование в работе систем электронного документооборота и электронных систем B2B-Center
1.3.6.1.4.1.24138.1.1.2.4	Использование в работе систем Федеральных ЭТП (Combo, 12 месяцев)
1.3.6.1.4.1.24138.1.1.2.6	Использование в работе систем Федеральных ЭТП (Combo, 15 месяцев)
1.3.6.1.4.1.24138.1.1.3.1	Пользователь системы электронного документооборота с органами государственной исполнительной власти
1.3.6.1.4.1.24138.1.1.8.8	Использование на электронных площадках, отобранных для проведения аукционов в электронной форме (3 месяца)
1.2.643.6.3	Использование в электронных торговых системах и в программном обеспечении, связанном с обменом электронными сообщениями
1.2.643.6.7	Использование в работе систем электронного документооборота и электронных систем B2B-Center
1.3.6.1.4.1.24138.1.1.8.1	Обеспечение юридической значимости в электронных торговых системах
1.2.643.6.15	Использование в работе систем ЭТП Фабрикант