

УТВЕРЖДЕН
Приказом ООО АйПиТелеком
№ ОКЗ-1а от 25 июля 2013 г.

Редакция от 06 июня 2016 г.

РЕГЛАМЕНТ

**оказания услуг Удостоверяющего центра по созданию
и выдаче квалифицированных сертификатов ключей
проверки электронных подписей ООО «АйПиТелеком»**

**Ульяновск
2016 г.**

СОДЕРЖАНИЕ

1. Сведения об Удостоверяющем центре	3
2. Термины и определения	4
3. Статус Регламента	6
4. Общее положение	6
5. Услуги, предоставляемые Удостоверяющим центром.	7
6. Вознаграждение Удостоверяющего центра, сроки и порядок расчетов	8
7. Предоставление информации	8
8. Права и обязанности сторон	9
9. Ответственность сторон	12
10. Разрешение споров	12
11. Порядок предоставления и пользования услугами Удостоверяющего центра.	13
12. Дополнительные положения	17
13. Список Приложений	
13.1. Приложение № 1 Форма подписного листа	
13.2. Приложение № 2 Образец формы заявления на регистрацию пользователя УЦ	
13.3. Приложение № 3 Форма доверенности представителя лица, проходящего процедуру регистрации	
13.4. Приложение № 4 Форма копии сертификата ключа проверки на бумажном носителе	
13.5. Приложение № 5 Форма заявление на подтверждение подлинности ЭП уполномоченного лица УЦ	
13.6. Приложение № 6 Форма заявления на аннулирование (отзыв, приостановление) сертификата ключа проверки электронной подписи	
13.7. Приложение № 7 Форма заявления на возобновление действия сертификата ключа проверки электронной подписи	
13.8. Приложение № 8 Форма заявления об отзыве согласия на обработку персональных данных	

1. Сведения об Удостоверяющем Центре

Общество с ограниченной ответственностью «АйПиТелеком» (ООО «АйПиТелеком»), именуемое в дальнейшем «Удостоверяющий Центр» (сокращенно - УЦ), организовано в соответствии с Уставом. Общество с ограниченной ответственностью «АйПиТелеком» зарегистрировано на территории Российской Федерации в городе Ульяновск. Свидетельство о регистрации № 3003469 от 10.01.02 г. регистрационной Палаты мэрии г.Ульяновска; Свидетельство о внесении записи в Единый государственный реестр юридических лиц серия 73 № 000714990, выдано «25» сентября 2002г. Инспекцией МНС России по Засвияжскому району г.Ульяновска, ОГРН 1027301481954.

Удостоверяющий Центр в качестве участника рынка услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании:

- Федерального закона 63-ФЗ «Об электронной подписи» от 6 апреля 2011 года;
- Лицензии УФСБ России по Ульяновской области ЛСЗ №0000252 Рег.73 от 12.11.2012г. на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

Юридический адрес: Российская Федерация, 432027, г.Ульяновск, ул.Радищева, д.143, корп.3

Адрес осуществления лицензируемого вида деятельности: 432017, г.Ульяновск, ул.Л.Толстого, д.54

Адрес для переписки: Российская Федерация, 432071, г.Ульяновск, а/я 2258

Банковские реквизиты:

- Ульяновский филиал ЗАО АКБ «Газбанк» г.Ульяновск

БИК 047308856, Р/с 40702810100000000734

К/с 30101810500000000856

Контактные телефоны, факс, адрес электронной почты:

тел./факс (8422) 248-000; e-mail: info@iptk.ru

2. Термины и определения

Заявитель - юридическое лицо независимо от организационно-правовой формы, физическое лицо или иной хозяйствующий субъект (в том числе индивидуальный предприниматель), обращающиеся в Удостоверяющий центр для получения квалифицированного сертификата ключа проверки электронной подписи и заключившие договор на оказание услуг Удостоверяющего центра.

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

Пользователь Удостоверяющего центра (далее **Пользователь УЦ**) - физическое лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец ключа проверки электронной подписи - юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи.

Рабочее время УЦ - промежуток времени с 08:00 по 17:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

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

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом 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 (далее - уполномоченный федеральный орган).

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

Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи) если:

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует на указанный момент времени.

Ключ проверки электронной подписи (далее - **Ключ проверки**) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Сертификат ключа проверки электронной подписи - 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.

Реестр сертификатов – реестр квалифицированных сертификатов ключей проверки электронной подписи, включающий в себя следующие разделы:

- реестр выданных квалифицированных сертификатов ключей проверки электронной подписи;
- реестр зарегистрированных владельцев квалифицированных сертификатов ключей проверки электронных подписей.

Список отозванных сертификатов (далее СОС) - электронный документ с электронной подписью удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы, действие которых прекращено и действие которых приостановлено.

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

Средство удостоверяющего центра – программное и (или) аппаратное средство, используемое для реализации удостоверяющим центром своих функций и соответствующее требованиям к средствам удостоверяющего центра, утверждённым Приказом ФСБ России от 29 декабря 2011 года № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

Стороны Регламента (далее – Стороны) – Удостоверяющий центр и пользователь, присоединившийся к настоящему Регламенту в порядке, определенном настоящим Регламентом.

Обработка заявления на аннулирование (отзыв) сертификата, приостановление/возобновление действия сертификата – совокупность действий по занесению сведений об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата в реестр Удостоверяющего центра и уведомлению Пользователя УЦ об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата.

Официальный публичный информационный сервер УЦ (далее – Сервер Удостоверяющего центра) - Официальный публичный информационный сервер УЦ, на котором публикуются корневой сертификат УЦ и актуальный список отозванных сертификатов размещен в Internet по адресу: <http://www.iptk.ru/>.

Удостоверяющий центр (далее УЦ) - ООО «АйПиТелеком» – юридическое лицо, осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи».

Электронная подпись (далее ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации)

или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Public Key Cryptography Standards (далее **PKCS**) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений.

3. Статус Регламента.

3.1. Настоящий Регламент разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

3.2. Регламент устанавливает общий порядок и условия предоставления Удостоверяющим центром пользователю, присоединившемуся к Регламенту в порядке, предусмотренном статьей 428 ГК РФ, услуг по изготовлению и выдаче сертификатов ключей проверки электронной подписи и дополнительных услуг, связанных с управлением сертификатами ключей проверки электронной подписи.

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

3.4. Настоящий Регламент распространяется: в форме электронного документа на сайте УЦ:

- по адресу: URL <http://iptk.ru/userfiles/file/reg-iptk.PDF>;

4. Общие положения

4.1. Присоединение к Регламенту

4.1.1. Производится путем подписания пользователем подписного листа к настоящему Регламенту, указанного в Приложении № 1 к настоящему Регламенту либо путем заключения между Удостоверяющим центром и пользователем гражданско-правового договора, предусматривающего присоединение пользователя к настоящему Регламенту.

4.1.2. Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, стороны вступают в соответствующие договорные отношения на неопределенный срок или, по желанию пользователя, на срок, указанный в Приложении № 1 к настоящему Регламенту или гражданско-правовом договоре, предусматривающем присоединение пользователя к настоящему Регламенту. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения, вносимые в Регламент, в соответствии с условиями настоящего Регламента.

4.1.3. Финансовые отношения устанавливаются согласно разделу 4 Регламента и Соглашения о договорной цене, сроком на 1 (Один) год. В случае обоюдного желания сторон продлить финансовые отношения по Регламенту, по окончании 1 (Одного) года работы, заключается новое Соглашение о договорной цене. В случае необходимости, новое Соглашение о договорной цене может быть заключено досрочно.

4.2. Порядок расторжения Регламента

4.2.1. Пользователь имеет право в одностороннем порядке расторгнуть настоящий Регламент, письменно уведомив об этом Удостоверяющий центр за 1 (Один) месяц до дня расторжения. Уведомление о расторжении Регламента, полученное Удостоверяющим центром от пользователя, является основанием для обязательного аннулирования сертификатов ключей проверки электронной подписи владельцев сертификатов ключей проверки электронной подписи уполномоченных данным пользователем. Датой аннулирования указанных сертификатов ключей проверки электронной подписи является дата расторжения настоящего Регламента. При этом Стороны до дня прекращения

действия Регламента обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с Регламентом.

4.2.2. Расторжение Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного расторжения, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

4.2.3. Любые справки по вопросам, связанным с оказанием услуг Удостоверяющего центра, предоставляются сотрудниками Удостоверяющего центра по телефону (8422) 248000 в рабочее время УЦ.

4.3. Применение Регламента.

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

4.3.2. В случае противоречия и/или расхождения названия какой-либо статьи со смыслом какого-либо пункта в ней содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

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

4.4. Изменения (дополнения) Регламента.

4.4.1. Внесение изменений (дополнений) в Регламент, в том числе в приложения к нему, может производиться Удостоверяющим центром только в части, не ограничивающей права пользователей УЦ, устанавливаемые разделом 6.2. Регламента.

4.4.2. Уведомление пользователей о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем размещения указанных изменений (дополнений) на сервере Удостоверяющего центра.

4.4.3. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент и не связанные с изменением действующего законодательства РФ, вступают в силу и становятся обязательными для Сторон по истечении 10 (десяти) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сервере Удостоверяющего центра.

4.4.4. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех пользователей УЦ, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

5. Услуги, предоставляемые Удостоверяющим центром.

5.1. Внесение в реестр Удостоверяющего центра регистрационной информации о пользователях УЦ.

5.2. Изготовление сертификатов ключей проверки электронных подписей пользователей УЦ в электронной форме.

5.3. Изготовление копий сертификатов ключей проверки электронной подписи пользователей УЦ на бумажном носителе.

5.4. Изготовление ключей электронной подписи пользователей УЦ.

5.5. Ведение реестра изготовленных сертификатов ключей проверки электронных подписей пользователей УЦ.

5.6. Предоставление копий сертификатов ключей проверки электронной подписи в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ.

5.7. Аннулирование (отзыв) сертификатов ключей проверки электронной подписи по обращениям пользователей УЦ. Форма заявления на аннулирование (отзыв) сертификата приведена в Приложении № 6 к Регламенту;

5.8. Приостановление и возобновление действия сертификатов ключей проверки электронной подписи по обращениям пользователей УЦ. Форма заявления на возобновление действия сертификата приведена в Приложениях № 6 и № 7 к Регламенту соответственно.

5.9. Предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах ключей проверки электронной подписи.

5.10. Подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ.

5.12. Распространение средств электронной подписи, оказание прочих услуг по обращениям пользователей Удостоверяющего центра.

6. Вознаграждение Удостоверяющего Центра, сроки и порядок расчетов.

6.1. УЦ осуществляет свою деятельность на коммерческой основе.

6.2. Стоимость и состав услуг УЦ публикуются на сервере УЦ.

6.3. Сроки и порядок расчетов за услуги, оказываемые УЦ, регулируются условиями договора между УЦ и пользователем УЦ.

6.4. УЦ безвозмездно представляет Сертификаты в форме электронных документов из Реестра выданных сертификатов УЦ, а также безвозмездно публикует СОС.

7. Предоставление информации

7.1. Удостоверяющий Центр предоставляет Пользователю УЦ по его письменному требованию:

7.1.1. Копию лицензии на право осуществлять деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

7.1.2. Копию сертификата соответствия на СКЗИ КриптоПро CSP версии 3.6.

7.2. Удостоверяющий центр при регистрации запрашивает у пользователя УЦ, а пользователь УЦ обязан предоставить Удостоверяющему центру документы, подтверждающие следующую информацию:

7.2.1. Наименование организации и основной государственный регистрационный номер, идентификационный номер налогоплательщика (предоставляются копии свидетельства о государственной регистрации и постановке на налоговый учет);

7.2.2. Лицензия, выданная пользователю, на право использования СКЗИ, в случае, если лицензия приобретена не в Удостоверяющем центре (предоставляется копия документа).

7.2.3. Место регистрации и адрес места жительства пользователя УЦ;

7.2.4. Сведения, необходимые для идентификации пользователя УЦ (или его представителя).

7.2.5. Для получения ключей и сертификатов ключей проверки электронных подписей пользователь УЦ (доверенное лицо) должен при себе иметь следующий комплект документов:

- основной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования заявителя - физического лица;
- документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя юридического лица (оригинал или копии, заверенные руководителем организации и печатью организации);
- надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);
- доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц.

7.3. Администратор УЦ выполняет процедуру идентификации личности заявителя, либо доверенного лица заявителя, путем установления личности, по основному документу удостоверяющего личность, а также проверку всех необходимых документов для изготовления ключей.

8. Права и обязанности Сторон.

8.1. Удостоверяющий центр обязан:

8.1.1. Предоставить Пользователю УЦ сертификат ключа проверки электронной подписи УЦ в электронной форме.

8.1.2. Использовать для создания ключа электронной подписи УЦ и формирования электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

8.1.2. Использовать ключ электронной подписи УЦ только для подписи издаваемых им сертификатов ключей проверки электронной подписи пользователей УЦ и списков отозванных сертификатов.

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

8.1.4. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Ульяновска. УЦ обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

8.1.5. Обеспечить регистрацию пользователей УЦ по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

8.1.6. Обеспечить уникальность регистрационной информации пользователей УЦ, используемой для идентификации владельцев сертификатов ключей проверки электронной подписи.

8.1.7. Прекратить, приостановить и возобновить действие сертификата ключа проверки электронной подписи Пользователя УЦ по соответствующему заявлению на прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

8.1.8. Прекратить действие сертификата ключа проверки электронной подписи Пользователя УЦ, если истек установленный срок, на который действие данного сертификата было приостановлено.

8.1.9. Прекратить действие сертификата ключа проверки электронной подписи Пользователя УЦ в случае нарушения конфиденциальности ключа электронной подписи

ПУЦ, с использованием которого был создан сертификат ключа проверки электронной подписи Пользователя УЦ.

8.1.10. Официально уведомить об аннулировании, прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в УЦ посредством публикации списка отозванных сертификатов.

8.1.11. Публиковать актуальный список отозванных сертификатов на сайте Удостоверяющего центра в ресурсе: <http://ca.ipk.ru/crl/iptelecom.crl> и <http://crl.ipk.ru/crl/iptelecom.crl>. Период публикации списка отозванных сертификатов – не более 1 месяца.

8.2. Сторона, присоединившаяся к Регламенту, обязана:

8.2.1. С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений Регламента до вступления их в силу не реже одного раза в неделю обращаться на сайт Удостоверяющего центра по адресу <http://ipk.ru/userfiles/file/reg-ipk.PDF> за сведениями об изменениях в Регламенте.

8.2.2. Пользователь УЦ обязан:

8.2.2.1. Обеспечить конфиденциальность ключей электронных подписей.

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

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

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

8.2.2.5. Немедленно обратиться в УЦ с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

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

8.2.2.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в УЦ по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

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

8.3. Пользователя УЦ обязан:

8.3.1. Хранить в тайне свой ключ ЭП, принимать всевозможные меры для предотвращения его потери, раскрытия, изменения или несанкционированного использования.

8.3.2. Не использовать для электронной подписи ключи ЭП, если ему известно, что эти ключи используются или использовались ранее другими лицами.

8.3.3. Использовать ключи ЭП только в соответствии с областями действия, указанными в соответствующем данному ключу сертификате ключа проверки электронной подписи.

8.3.4. Немедленно обратиться в УЦ с заявлением на аннулирование (отзыв) сертификата ключа проверки ЭП в случае, если стало известно, что эти ключи используются или использовались ранее другими лицами.

8.3.5. Не использовать ключ ЭП, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование (отзыв) которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата в УЦ по момент времени официального уведомления пользователя об аннулировании (отзыве) сертификата.

8.3.6. Не использовать ключ ЭП, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в УЦ по момент времени официального уведомления пользователя о приостановлении действия сертификата.

8.3.7. Не использовать ключ ЭП, связанный с сертификатом ключа проверки электронной подписи, который аннулирован (отозван) или действие его приостановлено.

8.4. Удостоверяющий центр имеет право:

8.4.1. Отказать в аннулировании (отзыве) сертификата ключа проверки электронной подписи пользователя УЦ в случае, если истек установленный срок действия ключа, соответствующего этому сертификату.

8.4.2. Отказать в приостановлении действия сертификата ключа проверки электронной подписи пользователя УЦ в случае, если истек установленный срок действия ключа, соответствующего этому сертификату.

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

8.4.4. Аннулировать (отозвать) сертификат ключа проверки электронной подписи пользователя УЦ в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) сертификата ключа проверки электронной подписи и указанием обоснованных причин.

8.4.5. Приостановить действие сертификата ключа проверки электронной подписи пользователя УЦ с уведомлением владельца сертификата ключа проверки электронной подписи, действие которого приостановлено, и указанием обоснованных причин.

8.4.6. Отказать в изготовлении сертификата ключа проверки электронной подписи пользователя УЦ в случае, если использованное пользователем УЦ для формирования запроса на сертификат ключа проверки средство криптографической защиты информации не поддерживается Удостоверяющим центром или пользователь УЦ не может предъявить Удостоверяющему центру лицензию на право использования СКЗИ.

8.5. Пользователь УЦ имеет право:

8.5.1. Применять сертификат ключа проверки электронной подписи УЦ для проверки электронной подписи УЦ в сертификатах ключей проверки электронных подписей, созданных УЦ.

8.5.2. Применять список отозванных сертификатов ключей проверки электронных подписей, созданный УЦ, для установления статуса сертификатов ключей проверки электронной подписи, созданных УЦ.

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

8.5.4. Получить копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную УЦ.

8.5.5. Обратиться в УЦ с заявлениями на выполнение УЦ действий, установленных настоящим Регламентом.

9. Ответственность сторон.

9.1. Сторона, не исполнившая или ненадлежащим образом исполнившая свои обязательства по настоящему Регламенту, несет ответственность за убытки, причиненные другой Стороне, в соответствии с действующим законодательством РФ.

9.2. 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.

9.3. УЦ не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях:

- если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлении пользователя УЦ;

- подделки, подлога либо иного искажения уполномоченным представителем пользователя УЦ либо третьими лицами информации, содержащейся в заявлении либо иных документах, предоставленных одной стороне от имени другой стороны.

9.4. Удостоверяющий центр несет ответственность за убытки при использовании ключа электронной подписи и сертификата ключа проверки электронной подписи пользователя УЦ, только в случае если данные убытки возникли при компрометации ключа УЦ либо вследствие несоответствий сведений в сертификате ключа проверки электронной подписи сведениям, указанным в Заявлении владельца сертификата ключа проверки электронной подписи.

9.5. В случае просрочки платежей в соответствии с Разделом 4 настоящего Регламента, Удостоверяющий центр может потребовать от пользователя выплаты в пользу УЦ пени из расчета ставки рефинансирования ЦБ РФ за весь период неисполнения обязательств.

В случае если Сторона проявит недобросовестность при исполнении своих обязательств по настоящему Регламенту, то другая сторона вправе публично известить об этом других пользователей.

Выплата пени и возмещение убытков не освобождает Стороны от выполнения обязательств по настоящему Регламенту.

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

10. Разрешение споров.

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

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

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

10.4. Сторона, получившая от другой Стороны претензию, обязана в течение 30 (Тридцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

10.5. Все споры и разногласия между Сторонами настоящего Регламента, возникающие из настоящего Регламента или в связи с ним и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде Ульяновской области.

11. Порядок предоставления и пользования услугами Удостоверяющего центра.

11.1. Создание сертификата ключа проверки электронной подписи

УЦ осуществляет создание сертификатов ключей проверки электронной подписи только тем лицам, которые присоединились к настоящему Регламенту и являются Стороной настоящего Регламента.

Создание сертификата ключа проверки электронной подписи осуществляется на основании заявления на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи. Форма заявления на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи приведена в Приложении №2 настоящего Регламента.

В случае создания сертификата ключа проверки электронной подписи юридическому лицу наряду с указанием в сертификате наименования юридического лица должно указываться физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Если ключи электронной подписи и сертификат ключа проверки электронной подписи юридического лица будут использоваться для автоматического создания электронных подписей, то физическое лицо может не указываться в сертификате ключа проверки электронной подписи.

Предоставление заявительных документов для создания сертификата ключа проверки электронной подписи, а также получение сформированных УЦ ключа электронной подписи и сертификата ключа проверки электронной подписи может быть осуществлено:

- для юридического лица:
 - физическим лицом, которое указывается в сертификате наряду с наименованием юридического лица;
 - физическим лицом на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложения №3 к настоящему Регламенту;
- для физического лица:
 - непосредственно этим физическим лицом;
 - физическим лицом на основании нотариально заверенной доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложения №3 к настоящему Регламенту.

Администратор УЦ на основе предоставленных заявительных документов выполняет действия по созданию сертификата ключа проверки электронной подписи. Сертификат ключа проверки электронной подписи записываются на предоставляемый заявителем ключевой носитель.

Администратор УЦ передает сформированный сертификат ключа проверки электронной подписи на ключевом носителе заявителю и по требованию заявителя распечатывает на бумажном носителе информацию, содержащуюся в созданном сертификате ключа проверки электронной подписи, по форме, приведенной в Приложения №4. Заявитель под расписку ознакамливается с информацией из сертификата ключа проверки электронной подписи.

Дополнительно, по согласованию с заявителем, Администратором УЦ сообщается ключевая фраза, используемая для аутентификации Пользователя УЦ при выполнении регламентных процедур, возникающих при нарушении конфиденциальности ключевых документов Пользователя УЦ.

Создание и выдача сертификатов ключей проверки электронной подписи УЦ осуществляется в день прибытия заявителя. День прибытия заявителя согласовывается с

Администратором УЦ. Удостоверяющий центр вправе отказать в создании сертификатов по заявлениям, поступившим в УЦ без согласования дня прибытия заявителя.

11.2. Изготовление и получение ключей электронной подписи и сертификата ключа проверки электронной подписи.

Выдача Сертификата физическому лицу осуществляется на основании заявления на изготовление Сертификата, подписанного Заявителем лично. Форма заявления на изготовление сертификата физическому лицу приведена в Приложении №2/2 к настоящему Регламенту.

11.2.1. В случае если физическое лицо не может прибыть лично в офис Удостоверяющего центра, на доверенное лицо, пребывающему в офис Удостоверяющего центра для получения ключа электронной подписи и сертификата ключа проверки электронной подписи, выписывается доверенность на получение ключа электронной подписи и сертификата ключа проверки электронной подписи соответствующего пользователю УЦ. Форма доверенности приведена в Приложении № 3 к настоящему Регламенту.

11.2.2. Выдача Сертификата юридическому лицу осуществляется на основании заявления на изготовление Сертификата, подписанного Уполномоченным представителем юридического лица. Форма заявления на изготовление Сертификата юридическому лицу приведена в Приложении №2/1 к настоящему Регламенту. Форма стандартной доверенности на Доверенное лицо юридического лица приведена в Приложении №3 к настоящему Регламенту

11.2.3. Сотрудник Удостоверяющего центра изготавливает две копии сертификата ключа проверки электронной подписи на бумажном носителе по форме определенной Приложением № 4 к настоящему Регламенту. Все копии сертификата ключа проверки электронной подписи на бумажном носителе заверяются собственноручной подписью пользователя УЦ и печатью пользователя, или собственноручной подписью доверенного лица.

11.2.4. По окончании процедуры изготовления ключей электронной подписи и сертификата ключа проверки электронной подписи пользователя УЦ или доверенному лицу выдаются:

- ключевой носитель, содержащий ключ электронной подписи;
- сертификат ключа проверки электронной подписи пользователя УЦ, соответствующий ключу электронной подписи (записывается на ключевой носитель).

11.2.5. В случае отказа в изготовлении сертификата ключа проверки электронной подписи пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

11.2.6. При принятии положительного решения, Администратор УЦ изготавливает сертификат ключа проверки электронной подписи и передает его пользователю УЦ.

11.2.7. Изготовление сертификата ключа проверки электронной подписи при внеплановой смене ключей пользователя УЦ осуществляется в следующих случаях:

- при компрометации ключа электронной подписи пользователя УЦ;
- при компрометации ключа электронной подписи уполномоченного лица УЦ;
- в случае если пользователь УЦ по каким-либо причинам не смог осуществить плановую смену ключей в установленные для этой процедуры сроки;
- в иных случаях, вызванных форс-мажорными обстоятельствами.

Изготовление сертификата ключа проверки электронной подписи при внеплановой смене ключей осуществляется аналогично процедуре изготовления первого сертификата пользователя УЦ.

11.3. Аннулирование (отзыв) сертификата ключа проверки электронной подписи.

11.3.1. Для осуществления аннулирования (отзыва) сертификата ключа проверки электронной подписи владелец ЭП подает заявление на аннулирование (отзыв) сертификата в Удостоверяющий Центр.

11.3.2. Аннулирование (отзыв) сертификата ключа проверки электронной подписи пользователя УЦ осуществляется Удостоверяющим Центром на основании письменного заявления, поступающего в Удостоверяющий Центр по форме, определенной Приложением № 6 к Регламенту.

11.3.3. Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи заверяется собственноручной подписью владельца сертификата, подписью и печатью пользователя и подается в офис Удостоверяющего Центра.

11.3.4. Обработка заявления на аннулирование (отзыв) сертификата и оповещение пользователя УЦ об аннулировании (отзыве) сертификата должны быть осуществлены не позднее 1 (Один) рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий Центр.

11.3.5. Временем аннулирования (отзыва) сертификата ключа проверки электронной подписи признается время официального уведомления пользователя УЦ об аннулировании (отзыве) данного сертификата.

11.4. Приостановление действия сертификата ключа проверки электронной подписи

11.4.1. Для осуществления приостановления действия сертификата ключа проверки электронной подписи владелец ЭП подает заявление на приостановление действия сертификата в Удостоверяющий центр.

11.4.2. Заявление в устной форме делается в офис Удостоверяющего центра по телефону (8422) 248-000. Заявитель должен сообщить сотруднику Удостоверяющего центра следующую информацию:

- идентификационные данные владельца сертификата ключа проверки;
- серийный номер сертификата, действие которого приостанавливается;
- срок, на который приостанавливается действие сертификата;
- ключевую фразу пользователя УЦ (определяемой в процессе регистрации пользователя УЦ).

11.4.3. Заявление принимается только в случае положительной аутентификации пользователя УЦ (совпадения ключевой фразы переданной в заявлении с информацией из реестра пользователей Удостоверяющего центра).

11.4.4. Заявление на приостановление действия сертификата ключа проверки электронной подписи заверяется собственноручной подписью владельца сертификата, подписью и печатью пользователя и подается в офис Удостоверяющего центра по форме, определенной Приложением № 6.

11.4.5. Обработка заявления на приостановление действия сертификата ключа и оповещение пользователя УЦ о приостановлении действия сертификата должны быть осуществлены не позднее 1 (Один) рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

11.4.6. Временем приостановления действия сертификата ключа проверки признается время официального уведомления пользователя о приостановлении действия данного сертификата.

11.4.7. В случае если в течение срока приостановления действия сертификата ключа проверки пользователя в Удостоверяющий центр не поступает заявление от пользователя о возобновлении действия сертификата, тогда сертификат аннулируется (отзывается) Удостоверяющим центром.

11.5. Возобновление действия сертификата ключа проверки электронной подписи.

11.5.1. Для осуществления возобновления действия сертификата ключа проверки электронной подписи владелец ЭП подает заявление на возобновление действия сертификата в Удостоверяющий центр.

11.5.2. Возобновление действия сертификата ключа проверки электронной подписи пользователя УЦ осуществляется Удостоверяющим центром на основании заявления,

поступающего в Удостоверяющий центр в бумажной форме. Заявление в бумажной форме подается в офис Удостоверяющего центра по форме, определенной Приложением № 7.

11.5.3. Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме заверяется собственноручной подписью владельца сертификата и подается в офис Удостоверяющего центра.

11.5.4. Обработка заявления на возобновление действия сертификата и оповещение пользователя УЦ о возобновлении действия сертификата должны быть осуществлены не позднее 1 (Один) рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

11.5.5. Временем возобновления действия сертификата ключа признается время официального уведомления пользователя УЦ о возобновлении действия данного сертификата.

11.5.6. Возобновление действия сертификата ключа проверки электронной подписи возможно только в течение срока, на который было приостановлено действие сертификата.

11.6. Подтверждение подлинности электронной подписи в электронных документах.

11.6.1. Для подтверждения подлинности электронной подписи в электронных документах, циркулирующих в рамках Услуг УЦ, пользователь УЦ подает заявление на подтверждение подлинности ЭП в электронном документе в УЦ.

11.6.2. Подтверждение подлинности ЭП электронного документа осуществляет УЦ на основании заявления в бумажной форме и содержащего следующую информацию:

- дата и время подачи заявления;
- наименование Услуги УЦ;
- идентификационные данные пользователя УЦ, ЭП которого требуется проверить в электронном документе;
- серийный номер сертификата открытого ключа, на котором требуется проверить ЭП электронного документа;
- дата и время формирования ЭП в электронном документе.

11.6.3. Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является текстовый файл на сменном магнитном носителе, содержащий в зависимости от выбранного режима и в соответствии с RFC 2311 (S/MIME Version 2 Message Specification) следующие структуры сообщений и content-types:

при использовании только подписи:

а) - письмо:

Content-Type: multipart/signed; protocol="application/pkcs7-signature"

Content-Transfer-Encoding: 7bit

- первая часть (исходные данные):

Content-Type: text/xml; charset=koi8-r

Content-Transfer-Encoding: base64

- вторая часть (подпись):

Content-Type: application/pkcs7-signature; name="smime.p7s"

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7s

или б) - электронный документ;

- файл с ЭП в формате BASE64.

при наличии подписи и шифрования:

а) - письмо:

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;

name=smime.p7m

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7m

- подписанные данные (т.е. MIME-part после расшифровки тела письма):
(используется подписывание без отделения подписи)

Content-Type: application/pkcs7-mime; smime-type=signed-data;
name=smime.p7m

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7m

или б) – электронный документ в виде файла в формате BASE64;

– файл с ЭП в формате BASE64.

11.6.4. Предоставляемые файлы электронных документов получают путем экспорта электронного документа, к которому применена электронная подпись, из программных продуктов, используемых пользователем УЦ.

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

- сертификат ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности электронной подписи, не утратил силу (действует) на момент формирования ЭП в электронном документе - дата и время формирования ЭП в электронном документе, указанная в заявлении на подтверждение подлинности ЭП;

- электронная подпись, проверенная на сертификате ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, верна;

- электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи – в поле Extended Key Usage;

- формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

11.6.6. Срок проведения работ по заявлению на подтверждение подлинности электронной подписи в электронном документе и предоставлению заключения о произведенной проверке составляет 5 (Пять) рабочих дней с момента его поступления в Удостоверяющий центр.

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

11.6.8. Результатом проведения работ по подтверждению подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра в письменной форме, подписанное всеми членами комиссии и заверенное печатью Удостоверяющего центра.

11.6.8. Заключение содержит:

- результат проверки электронной подписи электронного документа;

- отчет по выполненной проверке.

11.6.9. Отчет по выполненной проверке содержит:

- время и место проведения проверки;

- состав комиссии, осуществлявшей проверку;

- основание для проведения проверки;

- содержание и результаты проверки с указанием примененных методов;

- обоснование результатов проверки;

- данные, представленные комиссии для проведения проверки;

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

12. Дополнительные положения.

12.1. Плановая смена ключей УЦ

Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи УЦ выполняется в период действия ключа электронной подписи УЦ.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

– УЦ создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;

– УЦ создает новый сертификат ключа проверки электронной подписи.

Уведомление пользователей о проведении смены ключей УЦ осуществляется посредством публикации нового сертификата ключа проверки электронной подписи на сайте УЦ – <http://iptk.ru/userfiles/file/iptk.cer>

Старый ключ электронной подписи УЦ используется в течение своего срока действия для формирования списков отозванных сертификатов, создаваемых УЦ в период действия старого ключа электронной подписи УЦ.

12.2. Нарушение конфиденциальности ключевых документов УЦ, внеплановая смена ключей УЦ

В случае нарушения конфиденциальности ключа электронной подписи УЦ сертификат ключа проверки электронной подписи УЦ прекращает действие, Пользователи УЦ уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о нарушении конфиденциальности ключа электронной подписи УЦ на сайте УЦ.

Все сертификаты, подписанные с использованием ключа УЦ, конфиденциальность которого нарушена, считаются прекратившими действие.

После прекращения действия сертификата ключа проверки электронной подписи УЦ выполняется процедура внеплановой смены ключей УЦ. Процедура внеплановой смены ключей УЦ выполняется в порядке, определенном процедурой плановой смены ключей УЦ.

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

12.3. Нарушение конфиденциальности ключевых документов Пользователя УЦ

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

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Пользователь связывается с ПУЦ по телефону и приостанавливает действие сертификата, соответствующего ключу, конфиденциальность которого нарушена, посредством подачи заявления на приостановление действия сертификата в устной форме.

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

12.4. Конфиденциальность информации

12.4.1. Типы конфиденциальной информации

12.4.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи. УЦ не осуществляет хранение ключей электронных подписей Пользователей УЦ.

12.4.1.2. Персональная и корпоративная информация о Пользователях УЦ, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

12.4.2. Типы информации, не являющейся конфиденциальной

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

12.4.2.2. Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации открытой информации определяется УЦ.

12.4.2.3. Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной.

12.4.2.4. Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, создаваемые УЦ, относятся к общедоступным персональным данным.

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

12.4.3. Исключительные полномочия Удостоверяющего центра

12.4.3.1. Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях установленных законодательством Российской Федерации.

12.5. Хранение сертификатов ключей проверки электронной подписи в УЦ.

Срок хранения сертификата ключа проверки электронной подписи в УЦ осуществляется в течение всего периода его действия и 5 (Пять) лет после его прекращения действия. По истечении указанного срока хранения сертификаты ключей проверки электронной подписи переводятся в режим архивного хранения.

12.6. Прекращение оказания услуг/выполнения работ Удостоверяющим центром

12.6.1. В случае расторжения Регламента одной из Сторон действие всех сертификатов ключей проверки электронной подписи, владельцем которых является Сторона, присоединившаяся к Регламенту, по усмотрению УЦ может быть прекращено.

12.7. Непреодолимая сила (форс-мажор)

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

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

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

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

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

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

12.8. Архивное хранение

12.8.1. Архивному хранению подлежат следующие документы Удостоверяющего центра:

- аннулированные сертификаты ключей проверки уполномоченного лица УЦ;
- аннулированные сертификаты пользователей УЦ;
- заявления на регистрацию пользователей в УЦ;
- заявления на сертификат ключ проверки электронной подписи;
- заявления на аннулирование (отзыв) сертификатов ключей проверки;
- заявления на приостановление действия сертификатов ключей проверки;
- заявления на возобновление действия сертификатов ключей проверки;
- служебные документы Удостоверяющего центра.

12.8.2. Документы Удостоверяющего центра на бумажных носителях, в том числе и сертификаты ключей проверки электронной подписи пользователей на бумажном носителе, хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

12.8.3. Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов – 5 (Пять) лет.

12.8.4. Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой из числа сотрудников Удостоверяющего центра.

12.9. Структура сертификатов ключей проверки и списков отозванных сертификатов.

12.9.1. Удостоверяющий центр издает сертификаты ключей проверки пользователей УЦ в электронной форме формата X.509 версии 3 и список отозванных сертификатов (СОС) в электронной форме формата X.509 версии 2.

12.9.2. Структура сертификата ключа проверки уполномоченного лица УЦ.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CN = CS OU = Ulyanovsk department O = IPTelecom L = Ulyanovsk S = Ulyanovsk C = RU E = ca@iptk.ru
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = ФИО владельца OU = Название организации O = ООО «АйПиТелеком» L = Ульяновск C = RU E = e-mail владельца
Public Key	Ключ проверки	Ключ проверки (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		

Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) – сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение
Subject Key Identifier	Идентификатор ключа владельца сертификата 2.5.29.14	Идентификатор ключа уполномоченного лица Удостоверяющего центра, соответствующего данному сертификату
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL) 2.5.29.31	http://ca.ipk.ru/crl/iptelecom.crl

12.9.3. Структура списка отозванных сертификатов Удостоверяющего центра.

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = CS OU = Ulyanovsk department O = IPTelecom L = Ulyanovsk S = Ulyanovsk C = RU E = ca@ipk.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида: Серийный номер сертификата (CertificateSerialNumber) Время обработки заявления на аннулирование (отзыв) и приостановление действия сертификата (Time)
signatureAlgorithm	Алгоритм 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		
Reason Code	Код причины отзыва сертификата	"0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан СОС

12.9.4. Структура сертификата ключа проверки пользователя УЦ.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3

Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CN = CS OU = Ulyanovsk department O = IPTelecom L = Ulyanovsk S = Ulyanovsk C = RU E = ca@iptk.ru
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	SN = ФИО Пользователя УЦ Неструктурированное имя = ИНН Пользователя - КПП Пользователя - ИНН Пользователя УЦ CN = Наименование Пользователя O = Наименование Пользователя L = место регистрации Пользователя C = RU E = e-mail Пользователя
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость - невозможность осуществления отказа от совершенных действий; подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ 2.5.29.37	Набор идентификаторов (OID), определяющий отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение определенных Приложением № 10 к настоящему Регламенту
Subject Key Identifier	Идентификатор ключа владельца сертификата 2.5.29.14	Идентификатор ключа электронной подписи владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата 2.5.29.35	Идентификатор ключа электронной подписи уполномоченного лица УЦ, на котором подписан данный сертификат
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL) 2.5.29.31	http://ca.iptk.ru/crl/iptelecom.crl

СПИСОК ПРИЛОЖЕНИЙ

Приложение № 1 к Регламенту (Форма подписного листа)

Подписной лист к Регламенту услуг Удостоверяющего центра

_____ (полное наименование организации с указанием организационно-правовой формы), зарегистрированного по адресу: _____ (место нахождения, указанное в учредительных документах), в лице _____, действующего на основании _____,

1. Присоединяется к Регламенту оказания услуг Удостоверяющего центра в редакции № _____ от « _____ » д _____ 20__ г. (далее – Регламент) и является Стороной Регламента с момента передачи в ООО «АйПиТелеком» настоящего подписного листа.

2. Соглашается с тем, что изменения в Регламент вносятся в одностороннем порядке ООО «АйПиТелеком».

Дата передачи настоящего подписного листа ООО «АйПиТелеком» - «__» _____ 20__ г.

Наименование должности и Ф.И.О. единоличного исполнительного органа организации.

Подпись единоличного исполнительного органа организации.

Печать организации.

«Настоящим подтверждается, что данный подписной лист передан в ООО «АйПиТелеком» «__» _____ 20__ г.»

Генеральный директор
ООО «АйПиТелеком» _____

**Приложение №2 к Регламенту
Образец формы заявления на
регистрацию Пользователя УЦ**
(состав идентификационных данных
определяется областями использования сертификата)

Генеральному директору
ООО «АйПиТелеком»

Для юридических лиц

**Заявление
на создание сертификата ключа проверки электронной подписи**

_____ ,
(наименование организации, включая организационно-правовую форму, ОГРН, ИНН)

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

действующего на основании _____ просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи на предоставленный ключевой носитель для _____ (состав идентификационных данных определяется областями использования сертификата).

В качестве владельца сертификата ключа проверки электронной подписи наряду с указанием в сертификате наименования нашей организации прошу указать следующего полномочного представителя, действующего от имени нашей организации - пользователя Удостоверяющего центра:

_____ ,
(фамилия, имя, отчество полномочного представителя)

В сертификат ключа проверки электронной подписи прошу занести следующие идентификационные данные:

CommonName (CN)	Наименование организации или псевдоним
INN	ИНН организации
OGRN	ОГРН организации
Organization (O)	Наименование организации
Locality (L) StreetAddress (STREET) State (S) Contry (C)	Адрес места нахождения организации (согласно юридического или фактического адреса - по усмотрению заявителя) в виде: Город Улица, номер дома, корпуса, строения, пом. Наименование Субъекта РФ Страна=RU
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации (опционально)
GivenName (GN)	Имя и Отчество полномочного представителя (опционально)
Title (T)	Должность полномочного представителя (опционально)
OrganizationUnit (OU)	Наименование подразделения полномочного представителя (опционально)
E-Mail (E)	Адрес электронной почты полномочного представителя

_____ ,
(фамилия, имя, отчество пользователя)

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

соглашается с обработкой своих персональных данных ООО «АйПиТелеком» и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра
« _____ » _____ 201_____ г.

С Регламентом подчиненного удостоверяющего центра ООО «АйПиТелеком» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

М.П.

**Приложение №2/2 к Регламенту
Образец формы заявления на
регистрацию пользователя УЦ**
(состав идентификационных данных
определяется областями использования сертификата)

Генеральному директору
ООО «АйПиТелеком»

Для физических лиц

Заявление на создание сертификата ключа проверки электронной подписи
Я, _____

(фамилия, имя, отчество)

(серия и номер паспорта)

(кем и когда выдан)

прошу сформировать ключи электронной подписи и создать сертификат ключа проверки

электронный подписи на предоставленный ключевой носитель для _____ (состав идентификационных данных определяется областями использования сертификата)

В сертификат ключа проверки электронной подписи прошу занести следующие идентификационные данные:

CommonName (CN)	Фамилия Имя Отчество
SNILS	СНИЛС
SurName (SN)	Фамилия
GivenName (GN)	Имя и Отчество
Locality (L) StreetAddress (STREET) State (S) Contry (C)	Адрес места регистрации в виде: Город Улица, номер дома, корпуса, строение, квартира Наименование Субъекта РФ Страна=RU
INN	Личный ИНН (опционально)
E-Mail (E)	Адрес электронной почты (опционально)

Настоящим

(фамилия, имя, отчество)

что персональные данные, заносяемые в сертификаты ключей проверки электронной подписи, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра

(подпись)

« _____ » _____ 201 _____ г.

С Регламентом подчиненного удостоверяющего центра ООО «АйПиТелеком» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

**Приложение № 3 к Регламенту
Форма доверенности представителя
лица, проходящего процедуру
регистрации**

Доверенность №

« ____ » _____ 20__ г.

_____ (место составления)

_____ (полное наименование организации, включая организационно-правовую форму)
ИНН _____, ОГРН _____,
_____ (юридический адрес)

в лице _____
_____ (должность)

_____ (фамилия, имя, отчество полностью)
действующего на основании _____
_____ (указать наименование и реквизиты документа)

уполномочивает _____
_____ (фамилия, имя, отчество полностью)

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

1. Представить в Удостоверяющий центр ООО «АйПиТелеком» документы, необходимые для изготовления квалифицированного сертификата ключа проверки электронной подписи

_____ (Наименование юридического лица)
2. Получить сформированные ключи подписи и квалифицированный сертификат ключа проверки электронной подписи.

_____ (ФИО владельца сертификата полностью)
3. Подписать копию на бумажном носителе квалифицированного сертификата ключа проверки электронной подписи

_____ (ФИО владельца сертификата полностью)
Настоящая доверенность действительна по « ____ » _____ 20__ г.

Подпись владельца сертификата _____
_____ (подпись) _____ (инициалы, фамилия)

_____ (должность руководителя)

_____ (подпись)

_____ (расшифровка подписи)

М.П.

Приложение № 4 к Регламенту
Форма копии сертификата
ключа на бумажном носителе

Наименование организации - Удостоверяющего центра
Бланк сертификата ключа

Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Кому выдан:
Administrator 1
Кем выдан:
IPTELECOM CA Test
Действителен с 17 мая 2013 г. 13:51:00 UTC по 17 мая 2014 г. 14:01:00 UTC
Версия: 3 (0x2)
Серийный номер: 6127 DCC0 0000 0000 0038
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Издатель сертификата: CN = IPTELECOM CA Test, OU = DC, O = IPTELECOM., L = Ulyanovsk, C = RU, E = ca@iptk.ru
Срок действия:
Действителен с: 17 мая 2013 г. 13:51:00 UTC
Действителен по: 17 мая 2014 г. 14:01:00 UTC
Владелец сертификата: CN = Administrator 1, C = RU, E = ca@iptk.ru
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 3012 0607 2A85 0302 0224 0006 072A 8503 0202 1E01
Значение: 0440 C967 58E2 AA82 CA89 5BF2 9D9C 651D B2A8 D7FE C06C 32C5 D1E0 9446 9607 8E9D 4368 BA3C DC75
08DD 8470 9A49 6086 D056 9ADC ABB4 EB9E CFB2 2981 AB04 13CF B36E 393F
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: E0CC EFBB 8AAC 9A85 9814 F588 C6A1 4653 80D3 F0FB
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=2367 E1C2 A05C D442 F9E1 D82A AFC8 1E2A 3914 762A Поставщик сертификата:
Адрес каталога: CN= IPTELECOM CA Test OU=DC O=IPTELECOM= Ulyanovsk C=RU E= ca@iptk.ru Серийный номер
сертификата=7D18 EA1A E988 8898 454C 8D40 7A3C 2C27
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Значение: EAA3 CB2D 6E73 6F46 A1F8 0E72 5AB4 A92B 626A 3DF5 4A96 D093 7E15 1BD1 0D86 EFBD C074 88F8 A783
DB63 0FE8 AB9A CD9C 5129 BD2B C84B 4675 6EFD C482 D150 4D7B 0F75

Подпись владельца сертификата: _____/_____
" ____ " _____ 20__ г.

Средство криптографической защиты информации "КриптоПро CSP" v 3.6

Подписанный бланк сертификата ключа следует переслать по адресу: 432071, г. Ульяновск, а/я 2258

**Приложение № 5 к Регламенту
Форма заявление на подтверждение
подлинности ЭП уполномоченного
лица Удостоверяющего центра**

Генеральному директору
ООО «АйПиТелеком»

Для юридических лиц

**Заявление на подтверждение подлинности
электронной подписи уполномоченного лица Удостоверяющего центра**

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

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

действующего на основании _____

Просит подтвердить подлинность электронной подписи уполномоченного лица Удостоверяющего центра в изданном УЦ сертификате ключа подписи и установить его статус (действует/не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи, содержащий электронную подпись уполномоченного лица УЦ, на прилагаемом к заявлению машинном (оптическом) носителе – сер.№ XXXXX;

2. Время и дата, на момент наступления которых требуется установить статус сертификата:

« _____ : _____ » « _____ / _____ / _____ »
(час минута) (день месяц год)

Время и дата подачи заявления в УЦ:

« _____ : _____ » « _____ / _____ / _____ »
(час минута) (день месяц год)

_____ / _____ / _____
(должность руководителя организации) (подпись) (Ф.И.О.)

« _____ » _____ 20____ Г.
М.П.

**Приложение № 6 к Регламенту
Форма заявления на аннулирование
(отзыв, приостановление) сертификата**

Генеральному директору
ООО «АйПиТелеком»

**Заявление на аннулирование (отзыв, приостановление)
сертификата ключа**

Прошу аннулировать (отозвать, приостановить) сертификат ключа проверки электронной подписи серийный номер: _____,

выданный на имя _____
(Ф.И.О. владельца сертификата)

в связи с _____
(причина аннулирования (отзыва, приостановления) сертификата: компрометация, прекращение, повреждение носителя и т.д.).

М.П.

Владелец Сертификата _____
(подпись) (расшифровка подписи)

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) квалифицированного сертификата получено, личность

_____ (Ф.И.О.)

идентифицирована, сведения, указанные в Заявлении проверены.

Администратор Удостоверяющего центра: _____
(подпись) (расшифровка подписи)

**Приложение № 7 к Регламенту
Форма заявления на возобновление
сертификата ключа**

Генеральному директору
ООО «АйПиТелеком»

Заявление на возобновление сертификата ключа

Прошу возобновить действие сертификата ключа проверки электронной подписи серийный номер: _____,

выданный на имя _____
(Ф.И.О. владельца сертификата)

в связи с _____
(причина аннулирования (отзыва, приостановления) сертификата: компрометация, прекращение, повреждение носителя и т.д.).

М.П.

Владелец Сертификата _____
(подпись) (расшифровка подписи)

Настоящим подтверждаю, что Заявление на возобновление действия квалифицированного сертификата получено, личность:

(Ф.И.О.)

идентифицирована, сведения, указанные в Заявлении проверены.

Администратор Удостоверяющего центра: _____
(подпись) (расшифровка подписи)

**Приложение № 8 к Регламенту
Форма заявления об отзыве согласия
на обработку персональных данных**

Генеральному директору
ООО «АйПиТелеком»

**Заявление об отзыве согласия
на обработку персональных данных владельца сертификата ключа подписи
удостоверяющего центра**

Я, _____
(фамилия, имя, отчество)

(серия и номер паспорта)

(кем и когда выдан)

Прошу с «__» _____ 20__ года отозвать согласие на обработку персональных данных владельца сертификата ключа подписи.

Я ознакомлен с тем, что Согласие на обработку персональных данных, содержащихся в сертификатах ключей подписи, не может быть отозвано и действует до принятия решения о прекращении пользования услугами удостоверяющего центра.

Владелец СКП _____ / _____ /
подпись Ф.И.О

«__» _____ 20__ г.