

Утвержден

приказом директора ФГУ ФИПС

от 21.09.2010 № 304/44

РЕГЛАМЕНТ

Удостоверяющего центра

Федерального государственного учреждения

“Федеральный институт промышленной собственности Федеральной службы по интеллектуальной собственности, патентам и товарным знакам”

(Централизованная схема обслуживания)

1. Сведения об Удостоверяющем центре ФГУ ФИПС

1.1. Удостоверяющий центр ФГУ ФИПС, именуемый в дальнейшем «Удостоверяющим центром», является подразделением Федерального государственного учреждения "Федеральный институт промышленной собственности Федеральной службы по интеллектуальной собственности, патентам и товарным знакам" (ФГУ ФИПС) и осуществляет деятельность в рамках установленных полномочий от имени ФГУ ФИПС.

В своей деятельности Удостоверяющий центр руководствуется Положением об Удостоверяющем центре Федерального государственного учреждения «Федеральный институт промышленной собственности Федеральной службы по интеллектуальной собственности, патентам и товарным знакам», утвержденным приказом директора ФГУ ФИПС от 27.04.2007 № 75/44.

1.2. Удостоверяющий центр ФГУ ФИПС осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

- Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств;
- Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление распространения шифровальных (криптографических) средств;
- Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление предоставления услуг в области шифрования информации;
- Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

1.3. Сертификаты ключей подписей уполномоченного лица УЦ ФГУ ФИПС зарегистрированы Уполномоченным федеральным органом исполнительной власти Российской Федерации в части применения электронной цифровой подписи в Едином государственном реестре сертификатов уполномоченных лиц удостоверяющих центров, о чем получены соответствующие уведомления:

- Уведомление № 115 от 09 июня 2007 г. о регистрации в Едином государственном реестре сертификатов ключей подписей уполномоченных лиц удостоверяющих центров. Выдано Росинформтехнологией. Регистрационный номер записи П44-05-12-113 от 09 июня 2007 г.;
- Уведомление № 237 от 12 января 2009 г. о регистрации в Едином государственном реестре сертификатов ключей подписей уполномоченных лиц удостоверяющих центров. Выдано Росинформтехнологией. Регистрационный номер записи П44-05-12-236 от 12 января 2009 г.
- Уведомление № 356 от 03 декабря 2009 г. о внесении в Единый государственный реестр сертификатов ключей подписей Удостоверяющих центров. Выдано Росинформтехнологией. Регистрационный номер записи П44-05-12-356 от 03 декабря 2009 г.

Контактные телефоны, факс, адрес электронной почты:

тел./факс (495) 956-84-13 внутренний 62-48, 62-49;

e-mail: fipsca@rupto.ru.

Internet: www.fips.ru/certenroll/

2. Термины и определения

Администратор Удостоверяющего центра - ответственный работник Удостоверяющего центра ФГУ ФИПС, наделенный полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей и уполномоченный расписываться собственноручной подписью в сертификатах ключей подписей на бумажном носителе, изданных Удостоверяющим центром ФГУ ФИПС.

Владелец сертификата ключей подписи - физическое лицо, на имя которого Удостоверяющим центром ФГУ ФИПС выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключей подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи. Закрытый ключ электронной цифровой подписи действует на определенный момент времени (действующий закрытый ключ), если:

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

Компрометация ключа – наличие сомнений в том, что используемые ключи обеспечивают защиту информации в электронном документе. Примеры событий, связанных с компрометацией ключа:

- потеря ключевых носителей (в том числе с последующим их обнаружением);
- увольнение сотрудников, имевших доступ к ключевой информации;

- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- нельзя достоверно установить причину выхода из строя ключевого носителя (например, доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Маркер временного доступа - идентификатор (десятичное число) и секретный пароль (пятизначное символьное значение), предоставляющийся Пользователю и Оператору УЦ ФГУ ФИПС, не имеющим действующего закрытого ключа, для формирования и передачи в УЦ ФГУ ФИПС запроса на сертификат ключа подписи посредством веб-интерфейса, предоставляемого УЦ ФГУ ФИПС.

Оператор Службы актуальных статусов сертификатов – ответственный сотрудник УЦ ФГУ ФИПС, являющийся владельцем сертификата ключей подписи и соответствующего закрытого ключа, с использованием которого подписываются электронной цифровой подписью электронные ответы Службы актуальных статусов сертификатов.

Оператор Службы штампов времени – ответственный сотрудник УЦ ФГУ ФИПС, являющийся владельцем сертификата ключей подписи и соответствующего закрытого ключа, с использованием которого подписываются электронной цифровой подписью штампы времени.

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Пользователь Удостоверяющего центра – физическое лицо, зарегистрированное в УЦ ФГУ ФИПС.

Псевдоним владельца сертификата ключей подписи – вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в УЦ ФГУ ФИПС.

Регламент Удостоверяющего Центра ФГУ ФИПС (далее – Регламент)- документ, определяющий условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы УЦ ФГУ ФИПС.

Реестр УЦ ФГУ ФИПС – совокупность документов УЦ ФГУ ФИПС в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений о присоединении к Регламенту, изготовлении ключей подписи и сертификата ключей подписи;
- реестр зарегистрированных Пользователей Удостоверяющего центра;
- реестр заявлений на аннулирование (отзыв) сертификатов ключей подписей Пользователей Удостоверяющего центра;
- реестр заявлений на приостановление/возобновление действия сертификатов ключей подписей;
- реестр заявлений на подтверждение подлинности электронной цифровой подписи в электронном документе;
- реестр сертификатов ключей подписей Пользователей Удостоверяющего центра;
- реестр изготовленных списков отозванных сертификатов.

СКП (Сертификат ключа подписи) - документ на бумажном носителе или электронный документ с электронной цифровой подписью Уполномоченного лица УЦ ФГУ ФИПС, который включает в себя открытый ключ электронной цифровой подписи и который выдаётся УЦ ФГУ ФИПС участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключей подписи.

Сертификат ключа подписи действует на определенный момент времени (действующий сертификат), если:

- наступил момент времени начала действия сертификата ключей подписи;
- срок действия сертификата ключей подписи не истек;
- сертификат ключа подписи не аннулирован (отозван) и действие его не приостановлено.

Средства ЭЦП - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе,

- создание закрытых и открытых ключей электронных цифровых подписей.

Служба актуальных статусов сертификатов – сервис УЦ ФГУ ФИПС, обеспечивающий информирование пользователей о статусе сертификатов ключей подписей по протоколу OCSP (Online Certificate Status Protocol).

Служба Штампов времени электронного документа (штамп времени) – электронный документ, подписанный электронной цифровой подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью уполномоченного лица УЦ ФГУ ФИПС, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

Удостоверяющий центр ФГУ ФИПС (УЦ ФГУ ФИПС) (далее - Удостоверяющий центр) – Федеральное государственное учреждение “Федеральный институт промышленной собственности Федеральной службы по интеллектуальной собственности, патентам и товарным знакам”, изготавливающая сертификаты ключей электронной цифровой подписи в соответствии с Федеральным законом от 10 января 2002 г. №1-ФЗ «Об электронной цифровой подписи» и оказывающая иные услуги в области разработки, распространения и обслуживания шифровальных (криптографических) средств на основании лицензий, выданных Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов.

Услуги Удостоверяющего центра:

- создание ключей подписи;
- изготовление Сертификатов ключей подписи в форме документов на бумажных носителях и (или) в форме электронных документов;
- предоставление по запросам Потребителей услуг электронных копий сертификатов ключей подписи, зарегистрированных в Реестре сертификатов ключей подписи сертификатов Удостоверяющего центра;
- аннулирование (отзыв), приостановление и (или) возобновление действия сертификатов ключей подписи;
- предоставление по запросам Потребителей услуг сведений об аннулированных (отозванных) сертификатах ключей подписей и (или) о сертификатах, действие которых приостановлено;
- подтверждение подлинности электронных цифровых подписей в электронных документах.

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

ЭЦП (Электронная цифровая подпись) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключей подписи, а также установить отсутствие искажения информации в электронном документе.

Application Policy – набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в УЦ.

Authority Information Access - точки распространения ключа подписи Уполномоченного лица УЦ ФГУ ФИПС.

CRL Distribution point – поле в сертификате ключа подписи, содержащее точки распространения СОС.

Cryptographic Message Syntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений, описанный в документах RFC 3852 и RFC 3369. УЦ ФГУ ФИПС использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

Extended Key Usage - поле в сертификате ключа подписи, содержащее набор идентификаторов (OID), определяющих отношения, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.

NextUpdate – поле в СОС, в котором содержатся дата и время, по которое действителен СОС (дата и время издания следующего СОС).

OCSP-ответ – ответ сервера OCSP, содержащий статус запрашиваемого сертификата, на запрос клиента на получение статуса сертификата.

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

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. УЦ ФГУ ФИПС осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

ThisUpdate - поле в СОС, в котором содержится время издания СОС.

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

Validity Period – поле в сертификате ключа подписи, определяющее срок действия сертификата. Подразделяется на два подполя:

notBefore - время начало действия;

notAfter - время завершения действия.

3. Общие положения

3.1. Статус Регламента

3.1.1. Регламент Удостоверяющего центра Федерального государственного учреждения «Федеральный институт промышленной собственности Федеральной службы по интеллектуальной собственности, патентам и товарным знакам» (Удостоверяющий центр) (Централизованная схема обслуживания), именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

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

3.2. Присоединение к Регламенту

3.2.1. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным физическим лицом в Удостоверяющий центр Заявления на присоединение к Регламенту

Удостоверяющего центра ФГУ ФИПС, изготовление ключей подписи и сертификата Пользователя по форме Приложения №1 к настоящему Регламенту.

3.2.2. С момента регистрации Заявления на присоединение к Регламенту УЦ ФГУ ФИПС, изготовление ключей подписи и сертификата Пользователя физическое лицо, подавшее заявление, считается присоединившимся к Регламенту и является Стороной Регламента, далее Пользователем УЦ ФГУ ФИПС.

3.2.3. Факт присоединения физического лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления на присоединение к Регламенту УЦ ФГУ ФИПС, изготовление ключей подписи и сертификата Пользователя в реестре УЦ. Физическое лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

3.3. Порядок расторжения договорных отношений между присоединившейся Стороной и ФГУ ФИПС

3.3.1. Договорные отношения, возникшие между присоединившейся Стороной и ФГУ ФИПС после присоединения к Регламенту, могут быть расторгнуты по инициативе любой из Сторон при условии письменного уведомления другой Стороны за 30 календарных дней до предполагаемой даты прекращения договорных отношений. Договорные отношения считаются расторгнутыми после выполнения Сторонами своих обязательств.

3.3.2. 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).

3.4. Изменения (дополнения) Регламента

3.4.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится ФГУ ФИПС в одностороннем порядке.

3.4.2. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на сайте ФГУ ФИПС.

3.4.3. Все изменения (дополнения), вносимые ФГУ ФИПС в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении двух месяцев с даты размещения указанных изменений и дополнений в Регламенте на сайте ФГУ ФИПС.

3.4.4. Все изменения (дополнения), вносимые УЦ в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

3.4.5. 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 (дополнений) в силу.

3.4.6. Все приложения, изменения (дополнения) к настоящему Регламенту являются его составной и неотъемлемой частью.

3.5. Применение Регламента

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

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

4. Предоставление информации

4.1. УЦ ФГУ ФИПС предоставляет Стороне, присоединившейся к Регламенту, по ее требованию:

4.1.1. Копию лицензии ФСБ России на осуществление распространения шифровальных (криптографических) средств;

4.1.2. Копию лицензии ФСБ России на осуществление технического

обслуживания шифровальных (криптографических) средств;

4.1.3. Копию лицензии ФСБ России на осуществление предоставления услуг в области шифрования информации.

4.2. Удостоверяющий центр вправе запросить у Пользователя Удостоверяющего центра, а Пользователь Удостоверяющего центра обязан предоставить в Удостоверяющий центр документы, подтверждающие следующую информацию:

4.2.1. Сведения, необходимые для идентификации Пользователя Удостоверяющего центра: фамилия, имя, отчество, номер паспорта, кем и когда выдан.

4.2.2. Место регистрации и адрес места жительства Пользователя Удостоверяющего центра.

5. Права и обязанности Сторон

5.1. Удостоверяющий центр обязан:

5.1.1. Предоставить Пользователю Удостоверяющего центра сертификат ключей подписи Уполномоченного лица Удостоверяющего центра.

5.1.2. Использовать для изготовления закрытого ключа Уполномоченного лица Удостоверяющего центра и формирования электронной цифровой подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной цифровой подписи.

5.1.3. Использовать закрытый ключ Уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей подписей Удостоверяющего центра и списков отозванных сертификатов.

5.1.4. Принять меры по защите закрытого ключа Уполномоченного лица Удостоверяющего центра от несанкционированного доступа.

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

5.1.6. Зарегистрировать пользователя по заявлению на присоединение к Регламенту, изготовление ключей подписи и сертификата Пользователя в соответствии с порядком, определенным в настоящем Регламенте.

5.1.7. Занести регистрационную информацию Пользователя Удостоверяющего центра в реестр сертификатов ключей подписей Удостоверяющего центра и обеспечить уникальность регистрационной информации всех зарегистрированных в Удостоверяющем центре лиц, используемой для идентификации владельцев сертификатов ключей подписей.

5.1.8. Изготовить сертификат ключа подписи Пользователя Удостоверяющего центра по заявлению на изготовление ключей подписи и сертификата Пользователя и присоединение к Регламенту, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.9. Уведомить об изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра, владельца изготовленного сертификата ключей подписи.

5.1.10. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей подписей.

5.1.11. Обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей подписей.

5.1.12. Аннулировать (отозвать), приостановить и возобновить действие сертификата ключей подписи Пользователя Удостоверяющего центра по соответствующему заявлению на аннулирование (отзыв), приостановление и возобновление действия сертификата ключей подписи в соответствии с порядком, определенным в настоящем Регламенте.

5.1.13. Аннулировать (отозвать) сертификат ключей подписи Пользователя Удостоверяющего центра, если истек установленный срок, на который действие данного сертификата было приостановлено.

5.1.14. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра в случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра, с использованием которого был издан сертификат ключа подписи.

5.1.15. Публиковать актуальный список отозванных сертификатов на сайте <http://www.fips.ru/certenroll/cafips04.crl>. Периодичность публикации списка отозванных сертификатов Удостоверяющего центра – 1 месяц.

В случае аннулирования (отзыва) сертификата ключа подписи Пользователя или приостановления действия сертификата ключа подписи Пользователя, Удостоверяющий центр публикует список отозванных сертификатов содержащий сведения об отзыве/приостановлении, не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром

5.2. Пользователь Удостоверяющего центра обязан:

5.2.1. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

5.2.2. Применять для формирования электронной цифровой подписи только действующий личный закрытый ключ.

5.2.3. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

5.2.4. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключей подписи Пользователя Удостоверяющего центра (расширения Key Usage, Extended Key Usage, Application Policy сертификата ключей подписи).

5.2.5. Немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия сертификата ключей подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если Пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

5.2.6. Не использовать личный закрытый ключ, связанный с сертификатом ключей подписи, заявление на аннулирование (отзыв) которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата ключей подписи до момента официального уведомления об аннулировании (отзыве) сертификата ключей подписи.

5.2.7. Не использовать личный закрытый ключ, связанный с сертификатом ключей подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата ключей подписи до момента официального уведомления о приостановлении действия сертификата ключей подписи.

5.2.8. Не использовать личный закрытый ключ, связанный с сертификатом ключей подписи, который аннулирован (отозван) или действие которого приостановлено.

5.3. Удостоверяющий центр имеет право:

5.3.1. Отказать в регистрации и изготовлении сертификата ключей подписи в Удостоверяющем центре Пользователю Удостоверяющего центра, в случае ненадлежащего оформления необходимых регистрационных документов.

5.3.2. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключей подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв), приостановление и возобновление действия сертификата ключей подписи.

5.3.3. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключей подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего сертификату ключа подписи.

5.3.4. По согласованию с Пользователем Удостоверяющего центра приостановить действие сертификата ключей подписи Пользователя Удостоверяющего центра с указанием обоснованных причин.

5.3.5. Отказать в изготовлении сертификата ключей подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключей подписи средство криптографической защиты информации (средство электронной цифровой подписи) не поддерживается Удостоверяющим центром.

5.4. Пользователь Удостоверяющего центра имеет право:

5.4.1. Применять сертификат ключей подписи Уполномоченного лица Удостоверяющего центра для проверки электронной цифровой подписи Уполномоченного лица Удостоверяющего центра в сертификатах ключей подписей, изготовленных Удостоверяющим центром.

5.4.2. Применять список отозванных сертификатов ключей подписей, изготовленный Удостоверяющим центром, для установления статуса сертификатов ключей подписей, изготовленных Удостоверяющим центром.

5.4.3. Применять сертификат ключей подписи Пользователя Удостоверяющего центра для проверки электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в сертификате ключей подписи.

5.4.4. Применять носитель, поддерживаемый средством электронной цифровой подписи для хранения личного закрытого ключей.

5.4.5. Обратиться в Удостоверяющий центр с заявлением на присоединение к Регламенту, изготовление ключей подписи и сертификата Пользователя Удостоверяющего центра.

5.4.6. Обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) и приостановление действия сертификата ключей подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

5.4.7. Обратиться в Удостоверяющий центр с заявлением на возобновление действия сертификата ключей подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа и срока, на который действие сертификата было приостановлено.

5.4.8. Обратиться в Удостоверяющий центр за получением информации о статусе сертификатов ключей подписей Пользователей Удостоверяющего центра и их действительности на определенный момент времени.

5.4.9. Обратиться в Удостоверяющий центр за подтверждением подлинности электронной цифровой подписи в электронном документе, сформированной с

использованием сертификата ключей подписи, изданного Удостоверяющим центром.

6. Ответственность сторон

6.1. Стороны несут имущественную ответственность за невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту 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.

6.2. 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.

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

6.4. Удостоверяющий центр несет ответственность за убытки при использовании закрытого ключа подписи и сертификата ключей подписи Пользователя Удостоверяющего центра только в случае, если данные убытки возникли при компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра.

6.5. Вся ответственность по регистрации Пользователей Удостоверяющего центра, занесению данных в сертификаты ключей подписей, принятию решений по изготовлению и управлению сертификатами ключей подписей, формированию копий сертификатов ключей подписей Пользователей Удостоверяющего центра полностью возлагается на Удостоверяющий центр.

6.6. Возмещение убытков не освобождает Стороны от выполнения

обязательств в натуре.

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

7. Разрешение споров

7.1. Сторонами в споре, в случае его возникновения, считаются ФГУ ФИПС и Пользователь Удостоверяющего центра.

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

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

7.4. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в суде Москвы.

8. Порядок предоставления и пользования услугами Удостоверяющего центра

8.1. Регистрация Пользователя Удостоверяющего центра

Регистрация Пользователя Удостоверяющего центра осуществляется на основании Заявления на присоединение к Регламенту, изготовление ключей подписи и сертификата Пользователя по форме Приложения № 1 к настоящему Регламенту. Предоставление документов осуществляется лично Пользователем Удостоверяющего центра (либо его уполномоченным представителем с нотариально заверенной или заверенной печатью организации доверенностью по форме Приложения № 2) по предварительному согласованию с Администратором Удостоверяющего центра. Для регистрации в Удостоверяющем центре Пользователь Удостоверяющего центра предоставляет следующие документы:

- Заявление по форме Приложения № 1 Пользователя Удостоверяющего центра;
- документ, удостоверяющий личность Пользователя Удостоверяющего центра. Перечень документов указан в Приложении № 3 к настоящему Регламенту.

8.2. Генерация ключей, формирование первого сертификата ключей подписи Пользователя Удостоверяющего центра и плановая смена сертификата ключей подписи Пользователя Удостоверяющего центра

8.2.1. Пользователь предоставляет в Удостоверяющий центр Заявление на присоединение к Регламенту и изготовление ключей подписи и сертификата ключей подписи по форме Приложения №1 и носитель закрытого ключа, сертифицированный ФСТЭК, поддерживаемый средством ЭЦП и Удостоверяющим центром.

На основании предоставленного заявления Администратор Удостоверяющего центра осуществляет генерацию ключей подписи, запись закрытого ключа подписи на предоставленный носитель, изготовление сертификата ключей подписи, запись сертификата ключей подписи на предоставленный носитель и распечатывает по форме Приложения № 4 сертификат ключей подписи в двух экземплярах.

Два экземпляра сертификата ключей подписи Пользователя на бумажном носителе визируются Уполномоченным лицом Удостоверяющего центра, заверяются печатью Удостоверяющего центра и предоставляются Пользователю Удостоверяющего центра. Пользователь (либо его уполномоченный представитель) подписывает собственноручной подписью два экземпляра сертификата ключей подписи и один экземпляр возвращает Администратору Удостоверяющего центра.

8.3. Внеплановая смена ключей Пользователя Удостоверяющего центра

Внеплановая смена ключей осуществляется Пользователем Удостоверяющего центра в следующих случаях:

- при компрометации закрытого ключа Пользователя Удостоверяющего центра;
- при компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра;

Генерация ключей и формирование сертификата ключей подписи Пользователя Удостоверяющего центра осуществляется в соответствии с п. 8.2 настоящего Регламента.

8.4. Аннулирование (отзыв) сертификата ключей подписи Пользователя

Удостоверяющего центра

Удостоверяющий центр аннулирует сертификат ключа подписи Пользователя Удостоверяющего центра в следующих случаях:

- в случае прекращения действия настоящего Регламента в отношении Пользователя Удостоверяющего центра;
- по истечении срока, на который действие сертификата было приостановлено;
- по заявлению Пользователя Удостоверяющего центра;
- по истечении срока его действия;
- при компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра.

Удостоверяющий центр должен официально уведомить Пользователя и всех лиц, зарегистрированных в Удостоверяющем центре, об аннулировании (отзыве) сертификата ключей подписи не позднее одного рабочего дня с момента наступления описанного события.

Официальным уведомлением о факте отзыва сертификата ключей подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате и изданного не ранее времени наступления произошедшего случая. Временем отзыва сертификата ключей подписи признается время изготовления указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей в расширение `CRL Distribution Point` сертификата ключей подписи.

В случае аннулирования сертификата ключей подписи Пользователя Удостоверяющего центра по истечении срока его действия, временем аннулирования сертификата ключей подписи Пользователя Удостоверяющего центра признается время, хранящееся в поле `notAfter` поля `Validity Period` сертификата ключей подписи. В данном случае информация об аннулированном сертификате ключа подписи Пользователя Удостоверяющего центра в список отозванных сертификатов

не заносится.

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра временем аннулирования сертификата ключей подписи Пользователя Удостоверяющего центра признается время компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра, фиксирующееся в реестре изготовленных списков отозванных сертификатов Удостоверяющего центра. В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра информация о сертификате ключа подписи Пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

8.4.1. Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра по заявлению Пользователя Удостоверяющего центра.

Подача заявления на аннулирование (отзыв) сертификата ключей подписи осуществляется Пользователем Удостоверяющего центра по форме Приложения № 5 посредством почтовой или курьерской связи, либо при личном прибытии в Удостоверяющий центр.

После получения Удостоверяющим центром заявления на аннулирование (отзыв) сертификата ключей подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на отзыв сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в отзыве сертификата ключей подписи Удостоверяющий центр уведомляет об этом Пользователя Удостоверяющего центра.

При принятии положительного решения Администратор Удостоверяющего центра отзывает сертификат ключа подписи Пользователя Удостоверяющего центра.

8.5. Приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра

Удостоверяющий центр приостанавливает действие сертификата ключа подписи Пользователя Удостоверяющего центра в следующих случаях:

- по заявлению Пользователя Удостоверяющего центра в бумажной форме;
- по заявлению Пользователя Удостоверяющего центра в устной форме (по телефону) в случае компрометации или подозрения в компрометации закрытого ключа Пользователя Удостоверяющего центра;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

Действие сертификата ключей подписи Пользователя Удостоверяющего центра приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключей подписи составляет 15 дней.

Если в течение срока приостановления действия сертификата ключей подписи действие этого сертификата не будет возобновлено, то данный сертификат аннулируется (отзывается) Удостоверяющим центром.

Официальным уведомлением о факте приостановления действия сертификата ключей подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, и изданного не ранее времени наступления произошедшего случая. Временем приостановления действия сертификата ключей подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов. Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей в расширение CRL Distribution Point сертификата ключей подписи.

8.5.1. Приостановление действия сертификата ключей подписи Пользователя Удостоверяющего центра по заявлению в бумажной форме

Заявление на приостановление действия сертификата ключей подписи Пользователя Удостоверяющего центра оформляется по форме Приложения №6 к настоящему Регламенту и предоставляется в Удостоверяющий центр при личном прибытии. После получения Удостоверяющим центром заявления на

приостановление действия сертификата ключей подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого заявление было принято Удостоверяющим центром. В случае отказа в приостановлении действия сертификата ключей подписи Удостоверяющий центр уведомляет об этом Пользователя Удостоверяющего центра. При принятии положительного решения Администратор Удостоверяющего центра приостанавливает действие сертификата ключей подписи Пользователя Удостоверяющего центра.

8.5.2. Приостановление действия сертификата ключей подписи Пользователя Удостоверяющего центра по заявлению в устной форме

Приостановление действия сертификата ключей подписи по заявлению Пользователя Удостоверяющего центра в устной форме осуществляется исключительно при компрометации закрытого ключа или подозрении в компрометации закрытого ключа Пользователя Удостоверяющего центра.

Заявление подается в Удостоверяющий центр по телефону.

Пользователь Удостоверяющего центра должен сообщить Администратору Удостоверяющего центра следующую информацию:

- идентификационные данные, содержащиеся в сертификате ключа подписи, действие которого необходимо приостановить;
- серийный номер сертификата ключей подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключей подписи;
- ключевую фразу Пользователя Удостоверяющего центра (ключевая фраза предоставляется в процессе его регистрации).

Заявление Удостоверяющим центром принимается только в случае положительной аутентификации Пользователя Удостоверяющего центра (совпадения ключевой фразы с информацией из реестра зарегистрированных Пользователей

Удостоверяющего центра).

После принятия заявления Администратор Удостоверяющего центра принимает решение о приостановлении действия сертификата ключей подписи. Решения о приостановлении действия сертификата должно быть принято в течение рабочего дня поступления данного заявления.

В случае отказа в приостановлении действия сертификата ключей подписи Пользователь Удостоверяющего центра уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения Администратор приостанавливает действие сертификата открытого ключа. Не позднее 5 рабочих дней с момента приостановления действия сертификата ключей подписи Пользователь Удостоверяющего центра должен предоставить в Удостоверяющий центр заявление на приостановление, аннулирование (отзыв) сертификата ключей подписи в бумажной форме (в том случае, если факт компрометации закрытого ключа подтвердился), либо заявление на возобновление действия сертификата ключей подписи (в том случае, если компрометации закрытого ключа не было).

8.5.3. Приостановление действия сертификата ключей подписи по решению Удостоверяющего центра

Удостоверяющий центр вправе приостановить действие сертификата ключей подписи Пользователя Удостоверяющего центра в случаях компрометации или подозрения в компрометации закрытого ключа подписи Пользователя Удостоверяющего центра в том случае, если Пользователю Удостоверяющего центра не было известно о возможном факте компрометации ключей, а также в случаях неисполнения обязательств Пользователя Удостоверяющего центра по настоящему Регламенту.

После приостановления действия сертификата ключей подписи Администратор Удостоверяющего центра сообщает Пользователю Удостоверяющего центра о наступлении события, повлекшего приостановление действие сертификата, и уведомляет его о том, что действие сертификата Пользователя Удостоверяющего центра приостановлено.

8.6. Возобновление действия сертификата ключей подписи

Пользователя Удостоверяющего центра

Удостоверяющий центр возобновляет действие сертификата ключей подписи Пользователя Удостоверяющего центра только по заявлению Пользователя Удостоверяющего центра.

Подача заявления на возобновление действия сертификата ключей подписи осуществляется Пользователем Удостоверяющего центра по форме Приложения № 7 посредством почтовой или курьерской связи, либо при личном прибытии в Удостоверяющий центр.

Возобновление действия сертификата ключей подписи и официальное уведомление Пользователя и всех лиц, зарегистрированных в Удостоверяющем центре о возобновлении действия сертификата ключей подписи, должны быть осуществлены не позднее 5 рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

Официальным уведомлением о факте возобновления действия сертификата ключей подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления действия сертификата ключей подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изготовленные Удостоверяющим центром сертификаты ключей подписей в поле расширение CRL Distribution Point.

Возобновление действия сертификата ключей подписи возможно только в течение срока, на который действие сертификата ключей подписи было приостановлено.

8.7. Получение информации о статусе сертификатов ключей подписи, изготовленных Удостоверяющим центром

Информация о статусе сертификатов ключей подписи, изданных Удостоверяющим центром, предоставляется на основании заявления, направляемого Пользователем Удостоверяющего центра. Данное заявление оформляется по форме Приложения № 8 к настоящему Регламенту и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

- время и дата подачи заявления;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключей подписи;
- идентификационные данные Пользователя Удостоверяющего центра, статус сертификата ключей подписи которого требуется установить;
- серийный номер сертификата ключей подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключей подписи, которая предоставляется Пользователю Удостоверяющего центра. Предоставление Пользователю Удостоверяющего центра справки о статусе сертификата ключей подписи должно быть осуществлено не позднее 10 рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

8.8. Подтверждение подлинности электронной цифровой подписи в электронном документе

По желанию Пользователя Удостоверяющего центра Удостоверяющий центр проводит экспертные работы по подтверждению электронной цифровой подписи в электронном документе.

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

В данном случае для подтверждения подлинности электронной цифровой подписи в электронных документах Пользователь Удостоверяющего центра подает заявление в Удостоверяющий центр по форме, приведенной в Приложении № 9.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные Пользователя Удостоверяющего центра, подлинность электронной цифровой подписи которого необходимо подтвердить в электронном документе;
- время и дата формирования электронной цифровой подписи электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность электронной цифровой подписи.

Обязательным приложением к заявлению на подтверждение подлинности электронной цифровой подписи в электронном документе является магнитный носитель или иной носитель информации, содержащий:

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

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

Результатом проведения работ по подтверждению подлинности электронной цифровой подписи в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки подлинности электронной цифровой подписи электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

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.

Срок проведения работ по подтверждению подлинности электронной цифровой подписи в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет 10 рабочих дней с момента поступления заявления в Удостоверяющий центр.

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

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

- подтверждена подлинность электронной цифровой подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;
- сертификат ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности электронной цифровой подписи OCSP-ответа действителен;
- закрытый ключ подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- сертификат ключа подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении Extended Key Usage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);
- сертификат ключа подписи, статус которого установлен с использованием данного OCSP-ответа, издан Удостоверяющим центром и содержит в расширении Extended Key Usage или Application Policy область использования – Пользователь Службы актуальных статусов (1.2.643.2.2.34.26).

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – <http://ocsp.fips.ru/ocsp/ocsp.srf>. Указанный адрес заносится в расширение Authority Information Access (AIA) изготавливаемых Удостоверяющим центром сертификатов ключей подписей.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному электронной цифровой подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

- подтверждена подлинность электронной цифровой подписи Службы штампов времени (Оператора Службы штампов времени) в штампе времени;

- сертификат ключа подписи Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности электронной цифровой подписи штампа времени действителен;
- закрытый ключ подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампов времени действителен;
- сертификат ключа подписи Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);
- сертификат ключа подписи, на котором сформирована электронной цифровой подписи электронного документа и к которому относится данный штамп времени, издан Удостоверяющим центром и содержит в расширении Extended Key Usage или Application Policy область использования - Пользователь Службы штампов времени (1.2.643.2.2.34.25).

8.10. Прочие условия

Структуры сертификата ключей подписи Уполномоченного лица Удостоверяющего центра, ключа подписи Пользователя удостоверяющего центра и Списка отозванных сертификатов приведены в Приложениях № 10, 11, 12 соответственно.

9. Дополнительные положения

9.1. Компрометация ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа Пользователь Удостоверяющего центра связывается с Администратором Удостоверяющего центра по телефону и приостанавливает действие сертификата, соответствующего скомпрометированному ключу, посредством подачи заявления на

приостановление действие сертификата в устной форме (п. 8.5.2 настоящего Регламента).

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с п. 8.3 настоящего Регламента.

9.2. Конфиденциальность информации

9.2.1. Типы конфиденциальной информации

9.2.1.1. Закрытый ключ, соответствующий сертификату ключа подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра.

9.2.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в Удостоверяющем центре, не подлежащая непосредственной рассылке в качестве части сертификата ключей подписи, считается конфиденциальной.

9.2.2. Типы информации, не являющейся конфиденциальной

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

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

9.2.2.3. Информация, включаемая в сертификаты ключей подписей и списки отозванных сертификатов, изготавливаемых Удостоверяющим центром, не считается конфиденциальной.

9.2.2.4. Персональные данные, включаемые в сертификаты ключей подписей, изготавливаемых Удостоверяющим центром, относятся к общедоступным персональным данным.

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

9.2.3. Исключительные полномочия Удостоверяющего центра

9.2.3.1. Удостоверяющий центр имеет право раскрывать конфиденциальную

информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

Срок хранения сертификата ключей подписи в Удостоверяющем центре осуществляется в течение всего периода его действия и 5 лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты ключа подписи переводятся в режим архивного хранения.

9.3. Прекращение оказания услуг Удостоверяющим центром

В случае прекращения действия настоящего Регламента все сертификаты ключей подписей, владельцами которых являются Пользователи Удостоверяющего центра, аннулируются (отзываются) Удостоверяющим центром.

9.4. Форс-мажор

9.4.1. 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.

9.4.2. 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 программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

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

9.4.4. 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.

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

9.4.6. 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.

10. Вознаграждение Удостоверяющего центра.

10.1. Удостоверяющий Центр осуществляет свою деятельность на возмездной основе.

10.2. Стоимость, сроки и порядок расчетов за оказанные услуги Удостоверяющего Центра регулируются отдельными соглашениями между Удостоверяющим Центром и Пользователем УЦ.

10.3. Оплата осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на расчетный счет или иным способом, предусмотренным законодательством Российской Федерации.

10.4. В случае выполнения внеплановой смены ключей Уполномоченного лица Удостоверяющего Центра, Удостоверяющий Центр выполняет изготовление сертификатов ключей подписи Пользователей УЦ (в соответствии с процедурой, определенной Регламентом) безвозмездно.

11. Список приложений

- 11.1. Приложение №1. Заявление на присоединение к Регламенту и изготовление сертификата ключей подписи Пользователя Удостоверяющего центра
- 11.2. Приложение №2. Форма доверенности на получение ключей подписи и сертификата ключей подписи
- 11.3. Приложение №3. Перечень документов, удостоверяющих личность
- 11.4. Приложение №4. Бланк сертификата открытого ключа подписи на бумажном носителе
- 11.5. Приложение №5. Форма заявления на аннулирование (отзыв) сертификата ключей подписи
- 11.6. Приложение №6. Форма заявления на приостановление действия сертификата ключей подписи
- 11.7. Приложение №7. Форма заявления на возобновление действия сертификата ключей подписи
- 11.8. Приложение №8. Форма заявления на получение информации о статусе сертификата ключей подписи, изготовленного Удостоверяющим центром
- 11.9. Приложение №9. Форма заявления на подтверждение подлинности ЭЦП в электронном документе
- 11.10. Приложение №10. Структура сертификата ключей подписи Уполномоченного лица Удостоверяющего центра
- 11.11. Приложение №11. Структура сертификата ключей подписи Пользователя Удостоверяющего центра
- 11.12. Приложение №12. Структура Списка отозванных сертификатов Удостоверяющего центра

**Заявление на присоединение к Регламенту Удостоверяющего центра
ФГУ ФИПС, изготовление ключей подписи и сертификата Пользователя**

Я, _____
(Ф.И.О. заполняется печатными буквами)

прошу зарегистрировать меня в УЦ ФГУ ФИПС, изготовить сертификат, открытый, закрытый
ключи электронной цифровой подписи. Сообщаю о себе и прошу внести в сертификат ключа
подписи мои персональные данные и разрешаю их обработку:

Таблица заполняется печатными буквами

Должность (Т)		
Фамилия, Имя, Отчество (CN)		
Псевдоним		
Отдел (подразделение) (OU)		
Организация (O)		
Город (L)		
Область (S)		
Страна (регион) (C)		RU
Адрес электронной почты (E)		
Улучшенный ключ (Extended Key Usage)	Технические объектные идентификаторы	Защищенная электронная почта(1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
	Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение	

**Отдельно сообщаю о себе следующие сведения, не подлежащие
включению в сертификат ключа подписи:**

Документ удостоверяющий личность _____

Серия	
Номер	
Кем выдан	
Дата выдачи	

Извлечение из Федерального закона от 10 января 2002 г. №1-ФЗ «Об электронной цифровой подписи»

Статья 12. Обязательства владельца сертификата ключей подписи.

1. Владелец сертификата ключей подписи обязан:

- не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;
- хранить в тайне закрытый ключ электронной цифровой подписи;
- немедленно требовать приостановления действия сертификата ключей подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

2. При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключей подписи.

Приведенные выше сведения верны, со статьей 12 Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» ознакомлен.

В соответствии со статьёй 428 Гражданского Кодекса Российской Федерации полностью и, безусловно, присоединяюсь к действующему Регламенту, условия которого опубликованы в сети интернет www.fips.ru/certenroll/

С Регламентом Удостоверяющего центра «Федеральное государственное учреждение Федеральный институт промышленной собственности Федеральной службы по интеллектуальной собственности, патентам и товарным знакам» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

“ _____ ” _____ 20 ____ г. / _____
дата подпись

Настоящим подтверждаю, что Заявление на присоединение к Регламенту Удостоверяющего центра ФГУ ФИПС, изготовление ключей подписи и сертификата Пользователя получено, сведения, указанные в Заявлении, проверены.

Заявитель: _____

идентифицирован на основании документов, удостоверяющих личность.

Руководитель организации: _____
Должность И.О. Фамилия

М.П.

“ _____ ” _____ 20 ____ г. / _____
дата подпись

ПРИМЕЧАНИЕ:

*Форму заявления на присоединение к Регламенту Удостоверяющего центра ФГУ ФИПС, изготовление ключей подписи и сертификата Пользователя распечатывать на 1 листе с двух сторон.

* Наименование любого поля не должно превышать 64 символа, включая пробелы и знаки препинания (Для полей «Организация» и «Отдел» использовать краткое наименование).

* В поле «Адрес электронной почты», указывать только адрес рабочей электронной почты, если нет, поле оставить пустым

* Поле «Псевдоним» заполняется в случае изготовления Тестового сертификата (не именного), либо для изготовления сертификата на сервер

ДОВЕРЕННОСТЬ НА ПОЛУЧЕНИЕ КЛЮЧЕЙ ПОДПИСИ И СЕРТИФИКАТА КЛЮЧЕЙ ПОДПИСИ

г. _____ « _____ » _____ 20 ____ г.

Я, _____
(фамилия, имя, отчество пользователя)

Серия номер паспорта _____ / _____,

Кем и когда выдано _____,

уполномочиваю _____
(фамилия, имя, отчество)

Серия и номер паспорта _____ / _____

Кем и когда выдано _____

1. Предоставить в Удостоверяющий центр ФГУ ФИПС необходимые документы, определенные Регламентом Удостоверяющего центра ФГУ ФИПС, для изготовления ключей подписи, сертификата ключей подписи Пользователя Удостоверяющего центра ФГУ ФИПС
2. Получить сформированные ключи подписи и сертификат ключей подписи Пользователя Удостоверяющего центра ФГУ ФИПС

Представитель Пользователя наделяется правом расписываться на копии сертификата ключей подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью

Настоящая доверенность действительна по « _____ » _____ 20 ____ г.

Подпись уполномоченного представителя

Пользователя _____ / _____ /

Подтверждаю _____

**Перечень документов, удостоверяющих личность Пользователя
Удостоверяющего центра**

Документы, подтверждающие личность граждан Российской Федерации:

1. Паспорт гражданина Российской Федерации;
2. Заграничный паспорт гражданина Российской Федерации (паспорт, дипломатический паспорт или служебный паспорт);
3. Паспорт моряка (для лиц, работающих на судах заграничного плавания или на иностранных судах, курсантов учебных заведений);
4. Удостоверение личности военнослужащего Российской Федерации (для военнослужащих из состава офицеров, прапорщиков и мичманов на период пребывания на военной службе);
5. Военный билет военнослужащего (для лиц, которые проходят военную службу, для сержантов, старшин, солдат и матросов, а также курсантов военных образовательных учреждений профессионального образования);
6. Временное удостоверение личности, выдаваемое территориальным органом Федеральной миграционной службы;
7. Иные документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность.

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧЕЙ ПОДПИСИ

Прошу аннулировать (отозвать) сертификат ключа подписи, серийный номер:

выданный на имя _____

(ФИО владельца сертификата)

В СВЯЗИ С _____

(причина аннулирования (отзыва) сертификата ключей подписи:

компрометация закрытого ключа, прекращение работы и т.д.)

Владелец сертификата ключей подписи:

_____ / _____

Подпись / Расшифровка

« _____ » _____ 20__ г.

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключей подписи получено.

Заявитель _____
идентифицирован, сведения, указанные в Заявлении, проверены.

Уполномоченный сотрудник Удостоверяющего центра:

_____ / _____

Подпись / Расшифровка

« _____ » _____ 20__ г.

ЗАЯВЛЕНИЕ НА ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧЕЙ ПОДПИСИ

Прошу приостановить действие сертификата, серийный номер: _____

выданного на имя _____

(ФИО владельца сертификата)

в связи с _____

(причина приостановления действия сертификата ключей подписи)

Срок приостановления действия сертификата ключей подписи _____

(количество месяцев, дней прописью)

Владелец сертификата ключей подписи:

_____ / _____
Подпись / Расшифровка

« _____ » _____ 20__ г.

Настоящим подтверждаю, что Заявление на приостановление действия сертификата ключей подписи получено.

Заявитель _____
идентифицирован, сведения, указанные в Заявлении, проверены

Уполномоченный сотрудник Удостоверяющего центра:

_____ / _____
Подпись / Расшифровка

« _____ » _____ 20__ г.

ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧЕЙ ПОДПИСИ

Прошу возобновить действие сертификата ключей подписи, серийный номер: _____

выданного на имя _____

(ФИО владельца сертификата)

Владелец сертификата ключей подписи:

_____ / _____
Подпись / Расшифровка

« _____ » _____ 20__ г.

Настоящим подтверждаю, что Заявление на возобновление действия сертификата ключей подписи получено.

Заявитель _____
идентифицирован, сведения, указанные в Заявлении, проверены.

Уполномоченный сотрудник Удостоверяющего центра:

_____ / _____
Подпись / Расшифровка

« _____ » _____ 20__ г.

ЗАЯВЛЕНИЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СТАТУСЕ СЕРТИФИКАТА КЛЮЧЕЙ ПОДПИСИ, ИЗДАННОГО УЦ ФГУ ФИПС

Я, _____,
(ФИО подателя)

прошу предоставить информацию о статусе сертификата ключей подписи и
установить статус этого сертификата (действовал/не действовал) на момент:

_____ (дата и время, на момент наступления которых требуется установить статус сертификата)

Идентификационные данные пользователя, подлинность ЭЦП которого необходимо
подтвердить в электронном документе:

_____ (ФИО владельца сертификата, подвергаемого проверке)

_____ (серийный номер сертификата)

_____ (время и дата формирования ЭЦП электронного документа)

Заявитель (Пользователь Удостоверяющего центра):

_____ / _____
Подпись / Расшифровка

Время: _____ « _____ » _____ 20__ г.
дата

ЗАЯВЛЕНИЕ НА ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЭЦП В ЭЛЕКТРОННОМ ДОКУМЕНТЕ

Я, _____,
(ФИО подателя)

прошу подтвердить подлинность ЭЦП в электронном документе и установить статус
этого сертификата (действовал/не действовал) на момент:

(дата и время, на момент наступления которых требуется установить статус сертификата)

Идентификационные данные пользователя, подлинность ЭЦП которого необходимо
подтвердить в электронном документе:

(ФИО владельца сертификата, подвергаемого проверке)

(серийный номер сертификата)

(время и дата формирования ЭЦП электронного документа)

Заявитель (Пользователь Удостоверяющего центра):

_____/_____
Подпись / Расшифровка

Время: _____ « _____ » _____ 20 ____ г.
дата

**Структура сертификата ключей подписи Уполномоченного лица
Удостоверяющего центра**

“Федеральное государственное учреждение

**Федеральный институт промышленной собственности Федеральной службы по
интеллектуальной собственности, патентам и товарным знакам”**

Сертификат уполномоченного лица удостоверяющего центра

Сведения о сертификате:

Версия: 3

Серийный номер: 6058 A92B D8F6 82AD 43C3 E316 1C78 9641

Издатель сертификата: CN = FGU FIPS CA, OU = department 44, O = FEDERAL INSTITUTE OF INDUSTRIAL
PROPERTY, L = Moscow, C = RU, E = FipsCA@rupto.ru

Срок действия: Действителен с 19 ноября 2009 г. 8:30:54 UTC по 19 ноября 2039 г. 8:30:54 UTC

Серийный номер: 6058 A92B D8F6 82AD 43C3 E316 1C78 9641

Владелец сертификата: CN = FGU FIPS CA, OU = department 44, O = FEDERAL INSTITUTE OF INDUSTRIAL
PROPERTY, L = Moscow, C = RU, E = FipsCA@rupto.ru

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 3012 0607 2A85 0302 0223 0106 072A 8503 0202 1E01

Значение: 0440 4CD4 C217 74AE AD56 1F60 8A59 D040 F4EC 5412 CF35 08B6 FA02 0391 C854 A571 A321 CF7E
A637 8DE7 906F F5FE 3B9C 3E27 D107 0EAC C2D8 3550 02DD DDEF 8B60 DACE E3F5

Расширения сертификата X.509

1. Расширение 2.5.29.15

Название: Использование ключа

Значение: Цифровая подпись , Подписывание сертификатов , Автономное подписание списка отзыва (CRL) ,
Подписание списка отзыва (CRL)(86)

2. Расширение 2.5.29.19 (критическое)

Название: Основные ограничения

Значение: Тип субъекта=ЦС Ограничение на длину пути=Отсутствует

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: C538 19AD 5EAF 43AC EDA8 EB30 8D26 F862 DB54 FDC8

4. Расширение 1.3.6.1.4.1.311.21.1

Название: Версия ЦС

Значение: V1.1

5. Расширение 1.3.6.1.4.1.311.21.2

Значение: 0414 0667 7ECB 2A55 52C5 AF54 73AF 51DF 6AFA E4B4 9359

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2001

Идентификатор: 1.2.643.2.2.3

Значение: 20FE EE84 9694 4299 09CA 2B4E 6B4C 8D6C E13A 45FF 195A F019 D73B ED72 D9CF 06A9 1BA6
60EC 0C9B 284B 7949 6E83 C58B 16B2 600E 5C41 EDD1 3D10 00E7 7833 312E 0065

Средство криптографической защиты информации «КриптоПро CSP»

Сертификат выдал

/_____
подпись руководителя УЦ

« _____ » 20 ____ г.

М. П

Сертификат получил:

/_____
подпись уполномоченного лица УЦ

« _____ » 20 ____ г.

**Структура сертификата ключей подписи Пользователя
Удостоверяющего центра
“Федеральное государственное учреждение
Федеральный институт промышленной собственности Федеральной службы по
интеллектуальной собственности, патентам и товарным знакам”**

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	CommonName = FGU FIPS CA OU = department 44 O = FEDERAL INSTITUTE OF INDUSTRIAL PROPERTY L = Moscow C = RU E = fipsca@rupto.ru
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	CN = Общее имя = понятное пользователю имя SN = Фамилия = Фамилия Имя Отчество владельца UN = Неструктурированное Имя = идентификатор пользователя OU = Подразделение = наименование подразделения O = Организация = наименование организации L = Город = наименование населенного пункта S = Область = наименование субъекта Федерации C = Страна/Регион = RU E = Электронная почта = адрес электронной почты
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	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Цифровая подпись; Шифрование ключей; Шифрование данных
Extanded Key Usage	Улучшенный ключ	Пользователь Центра Регистрации, http, TLS клиент(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2) Защищенная электронная почта(1.3.6.1.5.5.7.3.4)
Application Policy	Политика применения	Идентификатор ключа центра сертификатов.
Subject Key	Идентификатор	Идентификатор закрытого ключа владельца сертификата

Idendifier	ключа владельца сертификата	
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа <i>Уполномоченного лица Удостоверяющего Центра</i> , которым подписан данный сертификат
CRL Distribution Points	Точки распространения списка отозванных сертификатов (CRL)	Точки распространения списков отозванных сертификатов, в виде http://www.fips.ru/certenroll/cafips04.crl
Authority Information Access	Адрес Службы актуальных статусов сертификатов	Точки распространения сертификата ключей подписи <i>Уполномоченного лица Удостоверяющего Центра</i> в виде http://www.fips.ru/certenroll/cafips04.cer

**Структура Списка отозванных сертификатов
Удостоверяющего центра
“Федеральное государственное учреждение
Федеральный институт промышленной собственности Федеральной службы по
интеллектуальной собственности, патентам и товарным знакам”**

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = FGU FIPS CA OU = department 44 O = FEDERAL INSTITUTE OF INDUSTRIAL PROPERTY L = Moscow C = RU E = FipsCA@rupto.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
Revoked Certificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (Serial Number) 2. Время обработки заявления на аннулирование (отзыв) или приостановление действия сертификата (Revokation Date) 3. Код причины отзыва сертификата (CRL Reason Code): «0» Не указана «1» Компрометация ключа «2» Компрометация ЦС «3» Изменение принадлежности «4» Сертификат заменен «5» Прекращение работы «6» Приостановление действия
Signature algorithm	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		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа <i>Уполномоченного лица Удостоверяющего Центра</i> , которым подписан СОС
CA Version	Версия сертификата издателя	Версия сертификата <i>Уполномоченного лица Удостоверяющего Центра</i>