2010

Регламент

Удостоверяющего центра

[Редакция 1.3]

ООО «Газинформсервис»
29.04.2010

Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»

РЕГЛАМЕНТ

УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

ООО «ГАЗИНФОРМСЕРВИС»

Редакция 1.3

г.Санкт-Петербург

2010г.

Оглавление

1. ВВЕДЕНИЕ

Настоящий документ описывает порядок предоставления услуг удостоверяющего центра и правила их использования участниками корпоративных информационных систем и информационных систем общего пользования.

Настоящий документ является соглашением, налагающим обязательства на все вовлеченные стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг удостоверяющего центра.

Регламент подготовлен в соответствии с рекомендациями RFC 3647. Certificate Policy and Certification Practices Framework.

1.1. Обзор

Настоящий документ определяет правила, механизмы и условия предоставления и использования услуг удостоверяющего центра, включая права, обязанности и ответственность владельцев и пользователей сертификатов ключей подписи, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, включая, но не ограничиваясь, такие операции, как выпуск, использование, обновление и отзыв сертификатов ключей электронной цифровой подписи.

1.2. Наименование и идентификация документа

Наименование документа: Регламент удостоверяющего центра общества с ограниченной ответственностью «ГАЗИНФОРМСЕРВИС».

Объектный идентификатор: не присвоен.

Версия документа: 1.3.

Дата: 29.04.2010

Актуальная редакция настоящего документа доступна по ссылке: http://ca.gaz-is.ru/repository/cps.pdf.

1.3. Участники

1.3.1. Удостоверяющий центр

Удостоверяющий центр – лицо, уполномоченное выдавать сертификаты ключей подписей в соответствии с законодательством.

1.3.2. Центр регистрации

Центр регистрации – лицо, уполномоченное УЦ проводить процедуру регистрации лиц, подавших заявления на выдачу сертификата ключа подписи, инициировать и рассматривать заявления на обновление и отзыв сертификатов от имени УЦ.

1.3.3. Владелец сертификата ключа подписи

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром 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).

1.3.4. Пользователь сертификата ключа подписи

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Пользователь сертификата ключа подписи может не являться владельцем сертификата ключа подписи.

1.3.5. Другие участники

Уполномоченный федеральный орган, осуществляющий ведение Единого государственного реестра сертификатов ключей подписей удостоверяющих центров в соответствии с приказом Федерального агентства по информационным технологиям №33 от 05.06.2006 .

1.4. Использование сертификатов ключей подписей

1.4.1. Допустимое использование сертификата ключа подписи

Сертификаты ключей подписей могут использоваться для электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в этих сертификатах.

1.4.2. Недопустимое использование сертификата ключа подписи

Сертификаты ключей подписей не должны использоваться в системах, критичных к отказоустойчивости, таких, как объекты ядерной энергетики, авиации и т.п.

1.5. Управление документом

1.5.1. Организация, ответственная за содержание документа

ООО «Газинформсервис»
198188, Россия, Санкт-Петербург, пр. Стачек, а/я 35.

1.5.2. Контактное лицо

Начальник отдела работы с абонентами удостоверяющего центра
ООО «Газинформсервис»
198188, Россия, Санкт-Петербург, пр. Стачек, а/я 35.
+7 (812) 3-052-052
ca@gaz-is.ru

1.5.3. Лица, утверждающие изменения

Изменения регламента утверждаются руководителем удостоверяющего центра.

1.5.4. Процедура утверждения изменений

Изменения в регламент вносятся сотрудниками удостоверяющего центра или Уполномоченным Федеральным органом и утверждаются руководителем удостоверяющего центра.

Официальным уведомлением участников информационных систем об утверждении изменений регламента является его публикация на интернет-сайте удостоверяющего центра по адресу: http://ca.gaz-is.ru/repository/cps.pdf.

Все изменения, вносимые в регламент, вступают в силу и становятся обязательными к исполнению всеми потребителями услуг удостоверяющего центра немедленно после их публикации.

1.6. Определения и сокращения

Удостоверяющий центр – лицо, выполняющее функции, предусмотренные Федеральным законом «Об электронной цифровой подписи»[1].

[1] Федеральный закон «Об электронной цифровой подписи»

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи[2].

СОС – список отозванных (аннулированных) сертификатов.

OCSP – online certificate status protocol, протокол онлайновой проверки статуса сертификата.

TSP – time stamping protocol, протокол меток времени.

2. ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1. Реестр выданных сертификатов

Удостоверяющий центр ведет реестр выданных сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем.

2.2. Публикация реестра выданных сертификатов

Удостоверяющий центр публикует реестр выданных сертификатов ключей подписей и осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Подтверждение подлинности электронной цифровой подписи производится путем предоставления сведений о статусе выданных сертификатов ключей подписей и сертификатов ключей подписей уполномоченных лиц удостоверяющего центра участникам информационных систем. Каждый сертификат ключа подписи, выданный удостоверяющим центром, содержит ссылку на раздел интернет-сайта, в котором опубликованы сертификаты ключей подписей уполномоченных лиц удостоверяющего центра и списки отозванных сертификатов.

Вышеуказанные сведения позволяют, при использовании сертифицированных средств электронной цифровой подписи, получать подтверждение подлинности электронной цифровой подписи в электронном документе автоматически. Сертифицированные средства электронной цифровой подписи так же позволяют получать сведения о фактах несанкционированных изменений электронных документов и уведомлять пользователей об отсутствии доверия к некорректным электронным цифровым подписям.

Сертификаты ключей подписей уполномоченных лиц удостоверяющего центра доступны на интернет-сайте удостоверяющего центра в разделе http://ca.gaz-is.ru/centre и на портале Уполномоченного Федерального органа.

2.3. Время и частота публикаций реестра

Выданные сертификаты ключей подписей вносятся в реестр и публикуются не позднее даты начала их действия.

Сведения о статусе сертификатов публикуются в соответствии с настоящим регламентом.

2.4. Доступ к реестру

Сведения, публикуемые на интернет-сайте удостоверяющего предоставляются участникам информационных систем в режиме свободного доступа с правами «только для чтения».

---

[2] Федеральный закон «Об электронной цифровой подписи»

Удостоверяющий центр осуществляет защиту от несанкционированного доступа к реестру.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. Имена (наименования)

3.1.1. Типы имен

Удостоверяющий центр выдает сертификаты ключей подписей, соответствующие стандарту ITU-T X.509v3. Выданные сертификаты содержат в полях «Субъект» и «Издатель» сведения, представленные в соответствии с рекомендациями ITU-T X.501 (Distinguished Names).

3.1.2. Необходимость в значимых именах (наименованиях)

Указанные в сертификатах ключей подписей Ф.И.О. физических точно совпадают со сведениями, указанными в предъявленных удостоверениях личности.

Указанные в сертификатах ключей подписей сведения ассоциированы с владельцем сертификата ключа подписи. Например, если в поле Common Name в качестве псевдонима указано DNS-имя веб-сервера, владельцем сертификата ключа подписи является ответственный за его эксплуатацию администратор.

3.1.3. Использование псевдонимов

В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи.

В случаях, когда сертификат явно не содержит фамилии, имени и отчества владельца в соответствующем поле, считается, что в этом сертификате ключа подписи указан псевдоним.

3.1.4. Правила интерпретации различных форм имен (наименований)

Нет условий.

3.1.5. Уникальность имен (наименований)

В случаях полного совпадения сведений, указываемых в нескольких сертификатах ключей подписей, принадлежащих разным владельцам, в них вносятся специальный атрибут (серийный номер), позволяющий однозначно идентифицировать их владельцев.

3.1.6. Использование торговых марок

Потребители услуг удостоверяющего центра обязаны не допускать использования в заявлениях на выдачу сертификатов ключей подписей торговых марок и другой интеллектуальной собственности, им не принадлежащей. Удостоверяющий центр не проверяет заявления на выдачу сертификатов ключей подписей на предмет содержания подобного рода. В случае возникновения споров о праве интеллектуальной собственности на сведения, содержащиеся в заявлениях или выданных сертификатах, удостоверяющий центр вправе отказать заявителю в выдаче сертификата или отозвать выданный сертификат, без объяснения причин.

3.2. Процедура первичной регистрации

3.2.1. Способ доказательства факта владения закрытым ключом

Заявитель должен продемонстрировать факт обладания закрытым ключом, соответствующим открытому ключу, который указан в заявлении и будет указан в сертификате. Способом доказательства владения закрытым ключом являются электронный документ формате PKCS#10.

В случае генерации ключевой пары удостоверяющим центром или центром регистрации, от имени заявителя, в его присутствии или в присутствии его законного представителя, доказательство факта обладания закрытым ключом не требуется.

3.2.2. Процедура аутентификации юридического лица

В тех случаях, когда заявление на выдачу сертификата ключа подписи предоставляется от имени юридического лица, заявитель предоставляет:

1. Выписку из ЕГРЮЛ, содержащая все сведения на юридическое лицо, полученная не позднее, чем за 1 (один) месяц до подачи заявки – оригинал или нотариально заверенная копия;

2. Дополнительные подтверждающие документы в случаях, указанных в п. 2. ст.9 Федерального закона «Об электронной цифровой подписи» от 10.01.2002 г. № 1-ФЗ.

Примечание: Выписка из ЕГРЮЛ может быть заменена предоставлением следующих документов:

- свидетельство о государственной регистрации юридического лица - нотариально заверенная копия;

- свидетельство о постановке на учет юридического лица в налоговом органе - нотариально заверенная копия;

- свидетельство о внесении записи в Единый государственный реестр юридических лиц - нотариально заверенная копия;

- устав с изменениями - нотариально заверенные копии;

- приказ (протокол) о назначении руководителя организации – оригинал или копия, заверенная руководителем организации.

3.2.3. Процедура аутентификации индивидуального предпринимателя

Если заявление подается от имени индивидуального предпринимателя, заявитель предоставляет:

1. Выписку из ЕГРИП, содержащая все сведения на индивидуального предпринимателя, полученная не позднее, чем за 1 (один) месяц до подачи заявки - оригинал или нотариально заверенная копия;

2. Дополнительные подтверждающие документы в случаях, указанных в п. 2. ст.9 Федерального закона «Об электронной цифровой подписи» от 10.01.2002 г. № 1-ФЗ.

Примечание: Выписка из ЕГРИП может быть заменена предоставлением следующих документов:

- свидетельство о государственной регистрации в качестве индивидуального предпринимателя - нотариально заверенная копия;

- свидетельство о постановке на учет в налоговом органе физического лица по месту жительства в Российской Федерации - нотариально заверенная копия.

3.2.4. Процедура аутентификации физического лица

При подаче заявления от физического лица, заявитель предоставляет:

1. Свидетельство о постановке на учет в налоговом органе физического лица по месту жительства в Российской Федерации - нотариально заверенная копия;

2. Копию паспорта – нотариально заверенная копия.

3.2.5. Сведения, указанные в заявлении, не подвергающиеся проверке

Нет условий.

3.2.6. Дополнительные условия аутентификации

Удостоверяющий центр оставляет за собой право осуществлять проверку сведений, указанных в заявлении на выдачу сертификата ключа подписи.

Удостоверяющий центр вправе требовать от заявителя представления дополнительных документов, подтверждающих сведения, указанные в заявлении.

3.2.7. Подтверждение полномочий владельца сертификата ключа подписи

В тех случаях, когда заявление на выдачу сертификата ключа подписи содержит наименование юридического лица или идентифицирующие его сведения, заявитель представляет в удостоверяющий центр соответствующую доверенность на осуществление юридических действий.

3.2.8. Взаимодействие с владельцами сертификатов ключей подписей, выданными другими удостоверяющими центрами

Владельцы сертификатов ключей подписей удостоверяющего центра ООО «Газинформсервис» могут быть участниками единого пространства доверия с владельцами сертификатов ключей подписей выданными другими удостоверяющими центрами в тех случаях, когда:

- между удостоверяющими центрами заключено соответствующее соглашение и приняты необходимые организационно-технические меры;
- владелец сертификата ключа подписи, выданного удостоверяющим центром ООО «Газинформсервис» является пользователем сертификата ключа подписи, выданного другим удостоверяющим центром.

3.3. Идентификация и аутентификация заявителя при смене ключей

Для непрерывного использования услуг удостоверяющего центра, владелец сертификата ключа подписи должен производить ежегодную плановую смену ключей и получать новый сертификат ключа подписи до момента окончания срока действия актуального сертификата. В соответствии с настоящим регламентом, сертификаты ключей подписей выдаются сроком на 1 (один) год. Не позднее, чем за две недели до истечения срока действия сертификата ключа подписи, его владелец должен подать заявление на выдачу нового сертификата ключа подписи.

3.3.1. Идентификация и аутентификация в случае плановой (очередной) смены ключей

Процедура аутентификации в случае плановой смены ключей может проводиться в порядке, описанном в п.3.2., либо на основании электронного документа, содержащего сведения заявления, заверенного действительной электронной цифровой подписью заявителя.

3.3.2. Идентификация и аутентификация в случае смены ключей после отзыва (аннулирования)

Процедура проводится в порядке, описанном в п. 3.2.

3.3.3. Идентификация и аутентификация заявителя при подаче заявления на отзыв (аннулирование) сертификата

До фактического выполнения процедуры отзыва сертификата ключа подписи, удостоверяющий центр проверяет тот факт, что заявление на отзыв сертификата исходит от лица, уполномоченного подавать заявления в соответствии с п.4.9.2.

4. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1. Заявление на выдачу сертификата ключа подписи

4.1.1. Лица, имеющие право подавать заявления на выпуск сертификатов ключей подписей

Заявление на выдачу ключа подписи имеют право подавать:
- физические лица или их законные представители;
- уполномоченные представители юридических лиц;

4.1.2. Процедура и обязательства по регистрации

Под регистрацией понимается внесение регистрационной информации о владельце сертификата ключа подписи в реестр.

Процедура регистрации владельца сертификата ключа подписи применяется в отношении физических лиц, обращающихся к услугам удостоверяющего центра в части изготовления сертификатов ключей подписей и/или изготовления закрытых и открытых ключей с записью их на ключевой носитель.

Лицо, желающее пройти процедуру регистрации должно подтвердить свое полное и безоговорочное присоединение к настоящему регламенту, а так же:
- заполнить и передать в удостоверяющий центр или центр регистрации заявление на выдачу сертификата ключа подписи, предоставив документально подтвержденные сведения;
- самостоятельно изготовить закрытый и открытый ключи подписи и передать в удостоверяющий центр или центр регистрации сообщение формата PKCS#10, содержащее открытый ключ, или присутствовать (обеспечить присутствие законного представителя) при выдаче ключей в удостоверяющем центре или центре регистрации;
- произвести оплату услуг удостоверяющего центра.

В случае подачи заявления на выпуск сертификата ключа подписи, содержащего персональные данные, владелец сертификата ключа подписи письменно выражает согласие с обработкой своих персональных данных удостоверяющим центром и признает, что персональные данные, вносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Заявление, поданные от физического лица, должны обязательно содержать следующие сведения:
- фамилию, имя и отчество;
- серия паспорта и номер паспорта;
- кем и когда выдан;
- адрес электронной почты;
- контактные телефоны.

Кроме этого, заявление, поданное от физического лица, представляющего юридическое лицо, должно обязательно содержать следующие сведения о юридическом лице:
- полное и сокращенное наименования, указанные в учредительных документах;
- должность и подразделение заявителя;
- данные доверенности (или других документов, подтверждающих правомочность действий от имени юридического лица);
- почтовый и юридический адрес;
- ИНН;
- КПП;
- банковские реквизиты;
- субъект Федерации, в котором зарегистрировано юридическое лицо.

По желанию заявителя, в заявлении может быть указан псевдоним.

4.2. Обработка заявления на выдачу сертификата ключа подписи

4.2.1. Процедура идентификации и аутентификации

Процедуры идентификации и аутентификации осуществляются в порядке, описанном в п.3.2.

4.2.2. Выдача и отказ в выдаче сертификата ключа подписи

Удостоверяющий центр выдает сертификат ключа подписи в случае успешного прохождения заявителем процедур идентификации и аутентификации, описанных в п.3.2. после подтверждения факта оплаты услуг.

Удостоверяющий центр вправе отказать заявителю в выдаче сертификата ключа подписи в случае невозможности подтверждения сведений, указанных в заявлении и/или при отсутствии подтверждения факта оплаты услуг удостоверяющего центра.

4.2.3. Сроки рассмотрения заявления на выдачу сертификата ключа подписи

Удостоверяющий центр обрабатывает заявления в коммерчески оправданные сроки. Как правило, срок обработки заявления не превышает одного рабочего дня. Время выдачи сертификата как правило не превышает 15 минут.

4.3. Изготовление сертификата ключа подписи

4.3.1. Действия удостоверяющего центра при изготовлении сертификата ключа подписи

Сертификат ключа подписи изготавливается оператором удостоверяющего центра в соответствии со сведениями, указанными в заявлении.

4.3.2. Уведомление заявителя о факте изготовления сертификата ключа подписи

Сертификат ключа подписи передается владельцу по адресу электронной почты, указанному в сертификате и публикуется в специальном разделе на интернет-сайте удостоверяющего центра.

4.4. Акцепт (признание) сертификата

4.4.1. Действия владельца сертификата ключа подписи, означающие акцепт сертификата

Следующие действия владельца сертификата ключа подписи означают акцепт сертификата:
- скачивание сертификата или его установка из полученного электронного документа;
- отсутствие у владельца мотивированных возражений (претензий) по поводу содержания сертификата ключа подписи.

4.4.2. Публикация сертификата

Удостоверяющий центр публикует реестр выданных сертификатов в соответствии с настоящим регламентом.

4.4.3. Уведомление пользователей удостоверяющего центра о выдаче сертификата ключа подписи

Официальным уведомлением пользователей удостоверяющего центра о выдаче сертификата ключа подписи является его публикация в реестре выданных сертификатов.

4.5. Использование ключей и сертификатов ключей подписи

4.5.1. Использование закрытого ключа и сертификата ключа подписи их владельцем

Использование владельцем закрытого ключа и сертификата ключа подписи допускается только после акцепта сертификата. Допускается использование сертификата строго в соответствии с указанными в нем сведениями.

4.5.2. Использование открытого ключа и сертификата ключа подписи пользователем

Пользователь сертификата ключа подписи должен использовать сертификат строго в соответствии с настоящим регламентом и сведениями, указанными в этом сертификате.

Получение дополнительных сведений и гарантий помимо указанных в сертификате ключа подписи осуществляется пользователем самостоятельно в случае необходимости.

До принятия решения о доверии к сертификату и/или электронной цифровой подписи, пользователь должен проверить:
- допустимость использования сертификата в соответствии со сведениями об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение;
- сведения о статусе сертификата ключа подписи;
- в тех случаях, когда сертификат отозван (аннулирован), или информацию о его статусе получить невозможно, пользователь должен самостоятельно принять решение об использовании такого сертификата; в этом случае все риски, связанные с доверием к такому сертификату несет пользователь.

4.6. Обновление сертификата ключа подписи

Обновление сертификата – процедура выдачи сертификата ключа подписи без изменения открытого ключа и сведений, указанных в сертификате.

В настоящее время указанная процедура не производится.

4.7. Смена ключей подписи

Смена ключей – процедура выдачи нового сертификата ключа подписи. Данная процедура подразумевает изготовление новых закрытого и открытого ключей подписи.

Процедура подачи заявления и выдачи сертификата при смене ключей полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки, за тем исключением, что заявление на выдачу нового сертификата ключа подписи может быть подана в электронном виде и заверено электронной цифровой подписью заявителя.

4.8. Изменение сведений, указанных в сертификате ключа подписи

Процедура подачи заявления и выдачи сертификата ключа подписи при изменении сведений, указанных в сертификате, полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки, за тем исключением, что заявление на изменение сведений, указанных в сертификате может быть подано в электронном виде и заверено электронной цифровой подписью заявителя.

4.9. Отзыв и приостановление действия сертификата

4.9.1. Условия отзыва сертификата

Удостоверяющий центр может отозвать сертификат ключа подписи и осуществить публикацию его в списке отозванных сертификатов в следующих случаях:
- получение от владельца сертификата ключа подписи заявления на отзыв сертификата;
- в удостоверяющий центр представлены доказательства нарушения владельцем сертификата ключа подписи условий настоящего регламента или обязательств перед другими участниками информационных систем;
- прекращение действия соглашения с владельцем сертификата ключа подписи;
- изменение сведений, указанных в сертификате.

4.9.2. Лица, уполномоченные подавать заявления на отзыв сертификатов ключей подписей

Заявление на отзыв сертификата ключа подписи может подавать только его владелец (в случае, если в сертификате указаны сведения о юридическом лице, от имени которого действует его владелец – руководитель этого юридического лица), удостоверяющие центры и центры регистрации, участвовавшие в процессе обработки заявлений на выдачу этих сертификатов.

4.9.3. Процедура подачи заявления на отзыв сертификата ключа подписи

Владелец сертификата ключа подписи связывается по телефону с удостоверяющим центром, подает устное заявление на отзыв сертификата и сообщает сотруднику удостоверяющего центра парольную фразу, полученную при выдаче сертификата.

После этого владелец сертификата ключа подписи должен направить в удостоверяющий письменное подтверждение устного заявления любым из перечисленных способов: в виде электронного сообщения, заверенного электронной цифровой подписью, по почте или курьерской службой доставки.

4.9.4. Срок подачи заявления на отзыв сертификата ключа подписи

Заявление на отзыв сертификата ключа подписи следует подавать в течение минимально возможного времени после появления такой необходимости (например в случае компрометации закрытого ключа).

4.9.5. Срок обработки заявления на отзыв сертификата ключа подписи

Удостоверяющий центр прилагает все коммерчески оправданные усилия для скорейшей обработки заявлений на отзыв сертификатов ключей подписей и публикации информации об отзыве этих сертификатов.

4.9.6. Требования к осуществлению проверки факта отзыва сертификата ключа подписи

Пользователь сертификата ключа подписи должен проверять факт отзыва сертификата, полагаясь на достоверность которого он собирается действовать. Проверка факта отзыва может осуществляться с использованием списков отозванных сертификатов или сервиса онлайновой проверки статуса сертификата, сведения о порядке доступа к которым указаны в каждом выданном удостоверяющим центром сертификате ключа подписи и настоящем регламенте.

4.9.7. Частота выпуска списков отозванных сертификатов

Списки отозванных сертификатов публикуются не реже одного раза в сутки.

Сертификаты с истекшим сроком действия, как правило, удаляются из списков отозванных сертификатов.

4.9.8. Задержка публикации списков отозванных сертификатов

Информация об отзыве сертификата ключа подписи публикуется, как правило, в течение нескольких минут после отзыва.

4.9.9. Возможность онлайновой проверки статуса сертификата

Информацию о статусе сертификата можно получить по протоколу онлайновой проверки статуса сертификата. Сведения о порядке доступа к сервису онлайновой проверки статуса сертификата включаются в выдаваемые сертификаты ключей подписей.

4.9.10. Требования к осуществлению онлайновой проверки факта отзыва сертификата

Пользователь сертификата ключа подписи должен самостоятельно осуществлять проверку статуса сертификата ключа подписи, полагаясь на достоверность которого он собирается действовать. В тех случаях, когда для определения степени доверия к сертификату недостаточно использования списков отозванных сертификатов, пользователь должен использовать сервис онлайновой проверки статуса сертификата.

В большинстве случаев рекомендуемые удостоверяющим центром для использования сертифицированные средства электронной цифровой подписи осуществляют вышеуказанные проверки автоматически.

4.9.11. Другие способы извещения участников информационных систем о фактах отзыва сертификатов

Нет условий.

4.9.12. Особые требования в случае компрометации ключей

Удостоверяющий центр прилагает все коммерчески оправданные усилия для оповещения участников информационных систем в случае компрометации ключей уполномоченных лиц удостоверяющего центра.

4.9.13. Условия приостановления действия сертификата

Нет условий.

4.9.14. Лица, уполномоченные подавать заявления на приостановление действия сертификатов

Нет условий.

4.9.15. Процедура подачи заявления на приостановление действия сертификата

Нет условий.

4.9.16. Ограничение срока приостановления действия сертификата

Нет условий.

4.10. Сервис онлайновой проверки статуса сертификата

4.10.1. Рабочие характеристики

Информация о статусах сертификатов доступна с использованием списков отозванных сертификатов и сервиса онлайновой проверки статуса сертификата.

4.10.2. Доступность службы проверки статусов сертификатов

Информация о статусах сертификатов доступна постоянно без запланированных перерывов в работе.

4.10.3. Дополнительные возможности

Нет условий.

4.11. Окончание пользования услугами удостоверяющего центра

Участник информационной системы может закончить использование услуг удостоверяющего центра путем расторжения соглашения о присоединении, путем отзыва своего сертификата(ов) или отказа от смены ключей после окончания их срока действия, при этом он не освобождается от ранее взятых на себя обязательствах перед другими удостоверяющим центром и участниками информационных систем.

4.12. Депонирование и восстановление ключей

Удостоверяющий центр не осуществляет депонирование ключей.

5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для обеспечения безопасности удостоверяющего центра применяются приведенные ниже меры, включающие в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а так же установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты от несанкционированного доступа. Этот контроль периодически выполняется администраторами безопасности на основе требований документации на средства защиты от несанкционированного доступа.

5.1. Физические меры обеспечения безопасности

5.1.1. Здания и сооружения

Удостоверяющий центр расположен таким образом, чтобы свести к минимуму возможность несанкционированного доступа, аварий и влияние природных явлений.

5.1.2. Физический доступ

Помещения удостоверяющего центра расположены в отдельном крыле четырехэтажного здания. Все помещения оборудованы системой контроля и управления доступом с идентификацией по смарт-картам, исполнительными устройствами системы контроля доступа электромеханического типа, системой видеонаблюдения.

Помещения удостоверяющего центра круглосуточно находятся под охраной выделенного подразделения.

Серверное и телекоммуникационное оборудование удостоверяющего центра размещено в выделенном специализированном помещении без окон.

Идентификационные карты для доступа в помещения УЦ выдаются сотрудникам по распоряжению руководителя удостоверяющего центра.

Посетители допускаются в помещения удостоверяющего центра только в назначенное им время в сопровождении персонала удостоверяющего центра.

5.1.3. Электроснабжение и кондиционирование воздуха

Технические средства удостоверяющего центра подключены к общегородской сети электроснабжения с использованием оборудования бесперебойного питания.

Электрические сети и электрооборудование, используемые в удостоверяющем центре, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Помещения удостоверяющего центра оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров

температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

5.1.4. Подверженность воздействию влаги

Защита оборудования удостоверяющего центра от влаги обеспечивается его размещением в специальных серверных шкафах.

5.1.5. Предупреждение и защита от возгорания

Помещения удостоверяющего центра оборудованы средствами пожаротушения в соответствии с требованиями, установленными законодательством Российской федерации.

5.1.6. Хранение архивных документов и электронных носителей

Документальный фонд удостоверяющего центра, как фондообразователя, хранится в соответствии с действующим законодательством по делопроизводству и архивному делу.

5.1.7. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками удостоверяющего центра, обеспечивающими документирование.

Важные документы и материалы подвергаются уничтожению в специальном оборудовании перед выбрасыванием.

5.1.8. Резервная площадка

Нет условий.

5.2. Организационные меры обеспечения безопасности

5.2.1. Разграничение ролей (полномочий)

Среди сотрудников удостоверяющего центра выделяют роли администратора, оператора, аудитора и системного администратора.

Администратор удостоверяющего центра осуществляет:
- управление деятельностью удостоверяющего центра и координация деятельности остальных служб;
- взаимодействие с участниками информационных систем в части разрешения вопросов, связанных с применением средств электронной цифровой подписи, ключей и сертификатов ключей подписей, изготавливаемых и распространяемых удостоверяющим центром;
- взаимодействие с участниками информационных систем в части разрешения вопросов, связанных с подтверждением электронной цифровой подписи уполномоченного лица удостоверяющего центра в сертификатах ключей подписей, изготовленных удостоверяющим центром в электронной форме, или подтверждения собственноручной подписи уполномоченного лица удостоверяющего центра в сертификатах открытых ключей, изготовленных удостоверяющим центром на бумажном носителе.

Оператор УЦ осуществляет:
- регистрацию заявлений;
- ведение реестра абонентов;
- распространение средств ЭЦП;
- изготовление криптографических ключей;
- изготовление и предоставление изготовленных сертификатов ключей подписей в электронной форме по обращению участников информационных систем;

- изготовление и предоставление сертификатов ключей подписей на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) сертификатов ключей подписей по обращениям их владельцев;
- предоставление участникам информационных систем сведений об аннулированных сертификатах ключей подписей;
- предоставление участникам информационных систем сертификатов ключей подписей, находящихся в реестре изготовленных сертификатов;
- техническое обеспечение процедуры подтверждения электронной цифровой подписи в документах, представленных в электронной форме, по обращениям участников информационных систем;
- техническое обеспечение процедуры подтверждения подлинности электронной цифровой подписи уполномоченного лица удостоверяющего центра, в изготовленных сертификатах открытых ключей, по обращениям участников информационных систем.

Системный администратор удостоверяющего центра осуществляет:
- организацию и выполнению мероприятий по эксплуатации программных и технических средств обеспечения деятельности удостоверяющего центра;

Аудитор осуществляет внутренний аудит деятельности УЦ.

5.3. Требования к персоналу

5.3.1. Квалификации персонала

Сотрудники удостоверяющего центра имеют высшее профессиональное образование, опыт работы в области информационной безопасности более 2 лет и прошли курсы повышения квалификации в области информационной безопасности с получением соответствующего сертификата.

5.3.2. Проверка биографии сотрудников

Проверка биографии сотрудников осуществляется в соответствии с внутренними инструкциями службы персонала удостоверяющего центра.

5.3.3. Требования к повышению квалификации персонала

Сотрудники удостоверяющего центра проходят курсы повышения квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

5.3.4. Требования к повторному прохождению обучения

В случае переноса средств удостоверяющего центра на новое оборудования или программное обеспечение, персонал удостоверяющего центра проходит курс обучения работе с новыми средствами.

5.3.5. Частота и последовательность смены деятельности сотрудников

Нет условий.

5.3.6. Ответственности за нарушения

Персонал удостоверяющего центра несет ответственность за свои действия в соответствии с законодательством РФ.

5.3.7. Требования к независимым подрядчикам

В исключительных случаях, когда для выполнения работ требуются услуги независимых подрядчиков, специалисты подрядчиков проводят работы только под наблюдением сотрудников удостоверяющего центра.

5.3.8. Документационное обеспечение персонала

Деятельность сотрудников удостоверяющего центра регламентирована внутренними инструкциями удостоверяющего центра.

Доступ сотрудников удостоверяющего центра к документам и документации, составляющей документальный фонд удостоверяющего центра, организован в соответствии с должностными инструкциями и функциональными обязанностями.

5.4. Порядок ведения записей аудита

5.4.1. Типы событий, подлежащих аудиту

Программно-аппаратный комплекс УЦ регистрирует следующие виды событий:

- системные события общесистемного программного обеспечения;

- принятие запроса на выпуск сертификат открытого ключа;

- выпуск сертификата открытого ключа;

- невыполнение внутренней операции программной компоненты;

- помещение запроса на сертификат;

- принятие запроса на сертификат;

- отклонение запроса на сертификат;

- выпуск списка отозванных сертификатов;

- невыполнение внутренней операции программной компоненты.

Структуры записей событий соответствуют эксплуатационной документации программного обеспечения реализации целевых функций удостоверяющего центра и общесистемного программного обеспечения.

5.4.2. Частота анализа журналов аудита

Журналы аудита еженедельно анализируются с целью обнаружения нарушений в работе программного и аппаратного обеспечения удостоверяющего центра, и анализа производительности систем.

В процессе анализа журналов аудита проводится расследование всех значительных нарушений работы и принимаются адекватные меры реагирования, которые в последствии документируются.

5.4.3. Срок хранения журналов аудита

Журналы аудита подлежат архивированию по истечении двух месяцев после окончания их анализа.

5.4.4. Защита журналов аудита

Журналы аудита защищены от просмотра, модификации и удаления средствами прикладного и общесистемного программного обеспечения.

5.4.5. Резервное копирование журналов аудита

Журналы аудита подлежат инкрементальному резервному копированию ежедневно и полному резервному копированию еженедельно.

5.4.6. Условия сбора записей аудита

События аудита автоматически записываются в журналы средствами прикладного и общесистемного программного обеспечения.

5.4.7. Уведомление субъекта события, вносимого в журнал аудита.

При записи события в журнал аудита, уведомление субъекта этого события не требуется.

5.4.8. Анализ уязвимостей

События, записываемые в журнал аудита, так же служат для анализа уязвимостей удостоверяющего центра. Удостоверяющий центр постоянно проводит анализ уязвимостей и предотвращает их возможные проявления. Все найденные уязвимости и принятые меры по их устранению включаются в ежегодный отчет об аудите.

5.5. Ведение архива

5.5.1. Типы архивных записей

Удостоверяющий центр ведет архив:

- журналов аудита в соответствии с п.5.4;

- соглашений с владельцами сертификатов ключей подписей, договоров;

- заявлений на выдачу и отзыв сертификатов ключей подписей.

5.5.2. Срок хранения архива

Удостоверяющий центр хранит архив на протяжении всего срока работы.

5.5.3. Защита архива

Удостоверяющий центр обеспечивает хранение архивных документов в соответствии с законодательством РФ.

5.5.4. Резервное копирование архива

Электронные носители архива подлежат инкрементальному резервному копированию ежедневно и полному резервному копированию еженедельно.

5.5.5. Требования к простановке времени создания архивных записей

Нет условий.

5.5.6. Условия архивирования

Удостоверяющий центр обеспечивает ведение архива в соответствии с законодательством РФ.

5.5.7. Порядок получения и проверки информации, хранящейся в архиве

Доступ к архиву имеют только уполномоченные сотрудники удостоверяющего центра. Целостность архива проверяется до извлечения сведений.

5.6. Смена ключей УЦ

Заблаговременно до окончания срока действия закрытого ключа уполномоченного лица удостоверяющего центра, администратор удостоверяющего центра производит формирование нового закрытого ключа и сертификата ключа подписи уполномоченного лица удостоверяющего центра.

Сформированный новый сертификат записывается на электронный носитель и передается уполномоченному лицу вместе с бланком сертификата.

По окончании действия закрытого ключа, ключевые носители с закрытым ключом и его копиями уничтожаются по акту комиссией.

Все владельцы и пользователи сертификатов ключей подписей обязаны получить новый сертификат удостоверяющего центра и добавить его в справочники сертификатов без удаления действующего сертификата удостоверяющего центра.

5.7. Восстановление в случае компрометации или аварии

5.7.1. Действия по предотвращению компрометации и аварии

Резервные копии данных удостоверяющего центра (реестры выпущенных сертификатов), ключей удостоверяющего центра, документационного обеспечения удостоверяющего центра помещаются в специально предназначенные для этих целей хранилища.

5.7.2. Случаи повреждения оборудования, программных и/или аппаратных сбоев

В случае повреждения оборудования, программных и/или аппаратных сбоев, сведения о происшествии поступают в службу безопасности удостоверяющего центра, которая доводит эти сведений до руководства удостоверяющего центра, расследует происшествие и принимает необходимые меры по устранению последствий и недопущению повторения подобных инцидентов.

5.7.3. Компрометация ключа участника информационной системы

В случае получения удостоверяющим центром информации о компрометации ключа от его владельца, служба безопасности, абонентский и технический отделы проводят расследование происшествия и принимают необходимые меры в соответствии с указаниями руководства удостоверяющего центра.

В случае необходимости отзыва (аннулирования) сертификата выполняется следующая процедура:

- сведения об аннулировании сертификата в связи с компрометацией доводятся до других участников информационных систем путем публикации в списке отозванных сертификатов;
- владелец скомпрометированного ключа письменно уведомляет других участников информационных систем о факте компрометации в случае необходимости;
- владелец скомпрометированного ключа получает новые ключи и сертификат в порядке, указанном в настоящем регламенте.

5.7.4. Восстановление работоспособности после аварии

Удостоверяющий центр имеет три резервные площадки в г. Санкт-Петербурге, в г. Москве и в г. Екатеринбурге.

План восстановления работоспособности после аварии предполагает восстановление в течение от 24 до 48 часов таких функций, как:

- выпуск сертификатов;
- отзыв сертификатов.

Публикация списков отозванных сертификатов и осуществляется непрерывно.

5.8. Разрешение конфликтных ситуаций

5.8.1. Некорректность входящего электронного документа или электронной цифровой подписи

Действия сторон в данной ситуации заключаются в следующем:

Принимающая сторона по телефону (или иным образом) запрашивает у отправляющей стороны информацию о документе, подлинность которого вызывает сомнения. При получении подтверждения об отправке указанного документа, запрашивает повторное оформление и отправку данного документа.

Результатом повторной обработки принимающей стороной (проверка электронной цифровой подписи) полученного документа может быть:

1. Повторная проверка дала отрицательный результат. Подпись документа неверна.

В этом случае делается вывод о возможном нарушении действующего криптографического ключа, либо о неисправности программно-аппаратных средств одной из сторон.

При этом необходимо:

- проверить сертификаты открытых ключей;

- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения СКЗИ. И переустановить его в случае необходимости.

Если положительного результата достигнуть не удалось, то необходимо обратиться в удостоверяющий центр.

2. Повторная проверка дала положительный результат. Подпись документа верна.

5.8.2. Непризнание отправителем электронного документа факта отправки документа, а также его целостности и подлинности

В случае если одна из сторон приходит к выводу, что другая сторона ссылается на документ, исходящий от первой, который не отправлялся и/или его содержание изменено, следует известить удостоверяющий центр о наличии конфликтной ситуации.

Удостоверяющий центр формирует Экспертную (согласительную) комиссию для разрешения конфликтной ситуации, в состав которой входят представители участников, вовлеченных в конфликтную ситуацию. Дополнительно могут привлекаться авторитетные, независимые специалисты в области криптографической защиты информации.

В ходе работы Экспертной комиссии рассматриваются документы, в том числе электронные, относящиеся к предмету разногласий, и выполняется процедура проверки ЭЦП документа. При этом могут быть использованы следующие эталонные данные:

- данные архива оригиналов принятых/отправленных документов;

- сертификаты ключей подписей, выданные Удостоверяющим Центром;

- дистрибутивы СКЗИ;

- ключевые носители.

Процедура проверки ЭЦП документа
Для проведения разбора конфликтной ситуации необходимы:

- заверенный удостоверяющим центром сертификат ключа подписи пользователя, подписавшего документ, подлинность или авторство которого оспаривается.

- файл, содержащий текст документа и электронную цифровую подпись его автора, в отношении которого возникает конфликтная ситуация.

Для разбора конфликтной ситуации необходимо выполнить следующие действия:

Произвести операцию проверки подписи электронного документа, авторство подписи которого оспаривается на рабочем месте Администратора УЦ.

Распечатать протокол проверки подписи.

Распечатать сертификат ключа подписи из Реестра удостоверяющего центра.

Сравнить представленный сертификат ключа подписи и распечатанный сертификат ключа подписи из Реестра удостоверяющего центра.

Авторство подписи под документом считается установленным, если совпадают открытые ключи представленного сертификата ключа подписи и сертификат ключа подписи из Реестра удостоверяющего центра, и в протоколе проверки подписи пользователя сформирована запись “Подпись верна”.

5.9. Прекращение работы удостоверяющего центра

В случае прекращения работы, удостоверяющий центр принимает все меры по минимизации влияния указанного процесса на участников информационных систем в соответствии с действующим законодательством.

6. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1. Изготовление и установка ключевой пары

6.1.1. Изготовление ключей

Изготовление ключей проводится лицом, подавшим заявление на выдачу сертификата ключа подписи самостоятельно или с помощью сотрудника удостоверяющего центра с использованием сертифицированных средств, рекомендованных для использования удостоверяющим центром.

В качестве ключевых носителей используются только носители, указанные в эксплуатационной документации средства, с помощью которых производится изготовление ключей.

6.1.2. Передача закрытого ключа подписи владельцу

В тех случаях, когда генерацию ключей производит сотрудник УЦ, процедура проводится в присутствии абонента или его законного представителя. Ключевой носитель с ключами

передается владельцу или его законному представителю сразу после выпуска и установки в него сертификата ключа подписи.

6.1.3. Передача открытого ключа подписи в удостоверяющий центр

В тех случаях, когда абонент осуществляет самостоятельную генерацию ключей, он передает в удостоверяющий центр открытый ключ подписи в составе сообщения формата PKCS#10 в электронном виде с использованием доступных каналов связи (напр. по e-mail или на электронном носителе).

6.1.4. Передача открытых ключей подписей участникам информационных систем

Удостоверяющий центр постоянно публикует сертификаты ключей подписей и списки отозванных сертификатов в соответствии с порядком, описанном в настоящем регламенте.

Сведения о публикации сертификатов ключей подписей уполномоченных лиц удостоверяющего центра содержатся в каждом выданном сертификате ключа подписи. Цепочки доверия, как правило, строятся программным обеспечением автоматически.

До начала использования сертификата ключа подписи участник информационной системы должен скачать и установить сертификаты ключей подписей уполномоченных лиц удостоверяющего центра.

Скачав и установив сертификаты ключей подписей уполномоченных лиц удостоверяющего центра, пользователь подтверждает свое присоединение к настоящему регламенту и полное и безоговорочное согласие с условиями использования сервисов удостоверяющего центра.

6.1.5. Размеры ключей

Размеры ключей электронной цифровой подписи:
- закрытый ключ – 256 бит;
- открытый ключ – 512 бит

Размеры ключей, используемых при шифровании:
- закрытый ключ – 256 бит;
- открытый ключ – 512 бит;
- симметричный ключ – 256 бит;

6.1.6. Параметры генерации и проверки качества закрытого ключа

Определяются сертифицированным СКЗИ автоматически.

6.1.7. Цели использования ключа (порядок заполнения поля key usage сертификата x.509v3)

Заполняются в соответствии с профилем сертификата (см. п. 7.2.1.).

6.2. Защита закрытого ключа, требования к ключевым носителям и криптографическим модулям

Все действия с ключевыми носителями должны осуществляться строго в соответствии с инструкциями по их эксплуатации и требованиями безопасности.

6.2.1. Требования к ключевым носителям

Допускается использование следующих типов носителей:
- ГМД 3,5’’;

- usb-flash;
- e-Token;
- смарт-карты РИК, Оскар, Магистра;
- идентификаторы Touch-Memory DS1995 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь";
- rutoken.

6.2.2. Закрытый ключ, контролируемый несколькими держателями (n из m)

В соответствии с эксплуатационной документацией средства криптографической защиты информации.

6.2.3. Депонирование закрытого ключа

Удостоверяющий центр не депонируют закрытые ключи.

6.2.4. Резервное копирование закрытого ключа

Резервное копирование закрытого ключа осуществляется владельцем самостоятельно. К резервной копии применяются те же требования, что и к оригиналу.

6.2.5. Архивирование закрытого ключа

Закрытые ключи с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией средства криптографической защиты информации. Архивное хранение закрытых ключей не допускается.

6.2.6. Запись закрытого ключа в криптографический модуль (ключевой носитель)

Производится автоматически средствами средства криптографической защиты информации в соответствии с эксплуатационной документацией.

6.2.7. Хранение закрытого ключа в криптографическом модуле (ключевом носителе)

Закрытые ключи хранятся только в зашифрованном виде.

6.2.8. Способы активации закрытого ключа

Все владельцы сертификатов ключей подписей обязаны хранить и защищать свои закрытые ключи подписей в соответствии с требованиями эксплуатационной документации средства криптографической защиты информации и действующим законодательством.

Активация закрытого ключа происходит при подключении ключевого носителя к персональному компьютеру с установленным необходимым для работы программным обеспечением после ввода PIN-кода.

6.2.9. Способы деактивации закрытого ключа

Закрытый ключ деактивируется средством криптографической защиты информации автоматически после выполнения связанных с его использованием операций или после физического отключения ключевого носителя от персонального компьютера.

6.2.10. Способы уничтожения закрытого ключа

Уничтожение закрытого ключа производится в соответствии с эксплуатационной документацией средства криптографической защиты информации.

6.2.11. Оценка криптографического модуля (ключевого носителя)

Ввиду невысокой надежности дискет и usb-flash, для хранения ключей рекомендуется использовать специализированные ключевые носители, такие, как eToken и Rutoken.

6.3. Другие особенности использования ключей электронной цифровой подписи

6.3.1. Архивирование открытых ключей подписей

Все сертификаты открытых ключей подписей архивируются в соответствии с порядком резервного копирования, установленном в удостоверяющем центре.

6.3.2. Сроки действия сертификатов и ключей

Срок действия закрытого ключа подписи уполномоченного лица удостоверяющего центра составляет 3 года. В течение 1 года 3 месяцев с момента начала срока действия закрытого ключа уполномоченного лица удостоверяющего центра, закрытый ключ используется для изготовления сертификатов ключей подписей и формирования списков отозванных сертификатов. По истечении 1 года 3 месяцев и до окончания срока действия закрытого ключа подписи уполномоченного лица удостоверяющего центра, данный закрытый ключ используется исключительно для формирования списков отозванных сертификатов. Срок действия сертификата ключа подписи уполномоченного лица удостоверяющего центра составляет 30 лет.

Сроки действия сертификатов сервисов актуальных статусов сертификатов и штампов времени составляют 25 лет.

Сроки действия закрытых ключей и сертификатов ключей подписей участников информационных систем составляют 1 год.

6.4. Данные активации закрытых ключей

6.4.1. Генерация и установка данных активации закрытого ключа

Данные активации (PIN-код), предназначенные для защиты ключевых носителей, как правило, устанавливаются на заводе-изготовителе. При генерации ключей сотрудник УЦ не меняет PIN-кода, установленного производителем.

К активационным данным (PIN) предъявляются следующие требования:
- смена должна быть произведена владельцем ключевого носителя немедленно после первого подключения к персональному компьютеру;
- не должен быть короче 8 символов;
- должен содержать минимум одну букву в нижнем регистре (строчную);
- должен содержать минимум одну букву, одну цифру и один знак препинания;
- не должен совпадать с именем учетной записи или датой рождения владельца;
- не должен содержать повторяющихся символов.

6.4.2. Защита данных активации закрытого ключа

Запрещается записывать PIN-код где-либо. PIN-код должен быть известен только владельцу ключа.

6.4.3. Особенности данных активации закрытого ключа

Нет условий.

6.5. Меры обеспечения информационной безопасности

Удостоверяющий центр имеет аттестаты соответствия требованиям по классу защищенности 1Г РД ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

В удостоверяющем центре выполняются требования нормативного документа «Временные требования к информационной безопасности удостоверяющих центров», утв. Первым зам. начальника ГУ безопасности связи ФАПСИ 24.01.2003 г.

Все участники информационных систем, использующие услуги удостоверяющего центра должны осуществлять эксплуатацию средств электронной цифровой подписи строго в соответствии с эксплуатационной документацией.

7. ПРОФИЛИ СЕРТИФИКАТОВ И CRL

7.1. Профиль сертификата

7.1.1. Версия сертификата

Удостоверяющий центр выдает сертификаты ключей подписей в электронной форме формата X.509 версии 3.

7.1.2. Расширения сертификата

Сертификаты ключей подписей содержат следующие дополнения:

authorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
subjectKeyIdentifier	Идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов
FreshestCRL	Точка распространения delta-CRL
KeyUsage	Назначение ключа

7.1.3. Объектные идентификаторы алгоритмов

Удостоверяющий центр использует следующие идентификаторы алгоритмов средства электронной цифровой подписи:

ГОСТ Р 34.10-2001	1.2.643.2.2.19
ГОСТ Р 34.11-94	1.2.643.2.2.9
ГОСТ 28147-89	1.2.643.2.2.21
Диффи-Хеллмана	1.2.643.2.2.98

7.1.4. Форматы имен (идентификационных данных)

В сертификатах ключей подписей поля идентификационных данных уполномоченного лица УЦ и владельца сертификата содержат атрибуты имени в формате X.500.

Сертификаты ключей подписей содержат следующие базовые поля X.509:

Signature:	Электронная цифровая подпись уполномоченного лица УЦ
Issuer:	Идентифицирующие данные уполномоченного лица УЦ
Validity:	Даты начала и окончания срока действия сертификата
Subject:	Идентифицирующие данные владельца сертификата ключа подписи
SubjectPublicKeyInformation:	Идентификатор алгоритма средства электронной цифровой подписи, с которыми используется данный открытый ключ, значение открытого ключа
Version:	Версия сертификата формата X.509 - версия 3
SerialNumber:	Уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов ключей подписей УЦ

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

Common Name	Фамилия, имя, отчество или Псевдоним
Organization	Наименование организации, являющейся владельцем УЦ
Email	Адрес электронной почты
Country	RU

Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом, являются:

Common Name	Фамилия, имя, отчество
Email	Адрес электронной почты
Country	RU

Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом и представляющего юридическое лицо, являются:

Common Name	Фамилия, имя, отчество
Organization	Наименование организации, которую представляет владелец сертификата
Organization Unit	Наименование подразделения организации, сотрудником которого является владелец сертификата
Email	Адрес электронной почты

Country	RU
State	Субъект Федерации, где зарегистрирована организация, , которую представляет владелец сертификата

7.1.5. Ограничения, накладываемые на имена (идентификационные данные)

На идентификационные данные налагаются ограничения по содержанию, длинам строк и используемым символам в соответствии с x.500.

7.1.6. Объектный идентификатор политики сертификата

Нет условий.

7.1.7. Использование расширения Policy Constraints

Нет условий.

7.1.8. Использование расширения Policy Qualifier

Нет условий.

7.1.9. Порядок обработки расширений Certificate Policies, имеющих пометку critical.

Решение о доверии к сертфикату ключа подписи принимается пользователем самостоятельно.

7.2. Профиль CRL

Удостоверяющий центр формирует списки отозванных сертификатов в электронной форме (CRL, COC) формата X.509 версии 2.

7.3. Дополнения CRL

Удостоверяющий центр ПК использует следующие дополнения:

Authority Key Identifier	Идентификатор ключа уполномоченного лица УЦ
Reason Code	Код причины отзыва сертификата открытого ключа

8. Приложение

Приложение №1 – Форма заявления на изготовление сертификата ключа подписи, на 2 листах

Приложение №2 – Форма доверенности, на 1 листе

Приложение № 3 – Форма заявления на отзыв сертификата ключа подписи, на 1 листе

Приложение №1

Форма Заявления на изготовление сертификата ключа подписи

Директору Удостоверяющего центра
ООО «Газинформсервис» Пушкину Н.А.
198188, г. Санкт-Петербург, пр. Стачек, д. 47

От _____
(Должность руководителя)

_____
(Название организации)

_____
(Фамилия И.О. руководителя)

_____
(ИНН/КПП организации)

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа подписи

1. Прошу сформировать ключи подписей и изготовить сертификаты ключей подписей в соответствии с указанными в настоящем заявлении идентификационными данными и сведениями об отношениях, при осуществлении которых электронные документы с электронной цифровой подписью будут иметь юридическое значение.

ФИО: _____
Должность: _____
Адрес e-mail: _____
Телефон: _____
Паспортные данные: _____
(серия, номер, кем и когда выдан) _____
Рабочее место _____
расположено по адресу _____
Операционная система: _____

Область применения сертификата:

ЭЦП будет использоваться в автоматизированной информационной системе (Система):

- ☐ государственного заказа Санкт-Петербурга
- ☐ государственного заказа Москвы
- ☐ ЭТП, входящих в АЭТП (sberbank-ast.ru, zakazrf.ru и др. - перечень на сайте: www.aetp.ru)
- ☐ ЕЭТП (roseltorg.ru)
- ☐ корпоративного электронного документооборота, организатором которого является _____ (указать наименование организации)

Ознакомлен с требованиями Регламента Удостоверяющего центра ООО «Газинформсервис» и приложениями к нему, в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.

В соответствии с Федеральным законом «О персональных данных» в целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО «Газинформсервис» (формирования общедоступных справочников сертификатов ключей подписей, списков отозванных сертификатов ключей подписей) своей волей и в своем интересе выражаю согласие ООО «Газинформсервис», расположенному по адресу: Российская Федерация, г. Санкт-Петербург, пр. Стачек, д. 47, на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) с использованием средств автоматизации или без использования таких средств моих персональных данных: фамилия, имя, отчество, адрес места жительства по паспорту, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), место работы, должность, служебный телефон. Согласие вступает в силу с момента его подписания, действует в течение 10 лет и может быть отозвано мною в любое время на основании моего письменного заявления.

Владелец сертификата ключа подписи: _____ _____
[личная подпись] Ф.И.О.

2. Администратором безопасности в организации Приказом № ____ от «___»_____20__ г. назначен:

ФИО: _____
Должность: _____
Адрес e-mail: _____
Паспортные данные: _____
(серия, номер, кем и когда выдан) _____
Телефон: _____

Ознакомлен с требованиями Регламента Удостоверяющего центра ООО «Газинформсервис» и приложениями к нему, в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к нему и обязуюсь соблюдать все его положения.

В соответствии с Федеральным законом «О персональных данных» в целях регистрации и обслуживания в информационной системе удостоверяющего центра ООО «Газинформсервис» (формирования общедоступных справочников сертификатов ключей подписей, списков отозванных сертификатов ключей подписей) своей волей и в своем интересе выражаю согласие ООО «Газинформсервис», расположенному по адресу: Российская Федерация, г. Санкт-Петербург, пр. Стачек, д. 47, на обработку им (включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) с использованием средств автоматизации или без использования таких средств моих персональных данных: фамилия, имя, отчество, адрес места жительства по паспорту, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи), место работы, должность, служебный телефон.

Согласие вступает в силу с момента его подписания, действует в течение 10 лет и может быть отозвано мною в любое время на основании моего письменного заявления.

Администратор безопасности: _____ _____
[личная подпись] Ф.И.О.

Руководитель организации:
Сведения представлены на основании подлинных документов и являются достоверными.

_____ _____ _____
(Должность руководителя организации) (подпись) (Фамилия И.О.)

«___» _____ 20__ г.

М.П.

Приложение №2

Форма Доверенности

ДОВЕРЕННОСТЬ №_____

Дата выдачи «___» _____ 20__ г.

Действительна по «___» _____ 20__ г.

Я, _____

(ФАМИЛИЯ Имя Отчество)

_____

(Должность, название организации)

Паспорт _____ _____

(Серия) (Номер)

Кем выдан _____

Дата выдачи _____

ДОВЕРЯЮ

_____

(ФАМИЛИЯ Имя Отчество)

_____

(Должность, название организации)

Паспорт _____ _____

(Серия) (Номер)

Кем выдан _____

Дата выдачи _____

ПРЕДСТАВЛЯТЬ МОИ ИНТЕРЕСЫ В УЦ ООО «ГАЗИНФОРМСЕРВИС», А ИМЕННО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

- вместо меня присутствовать при создании ключей моей электронной цифровой подписи (ЭЦП) и запроса на сертификат ключа подписи;
- получить ключевой носитель, содержащий:
  - ключевые файлы в контейнере;
  - сертификат ключа подписи;
- получить мой сертификат ключа подписи на бумажном носителе;
- расписаться за меня в Сертификате ключа подписи на бумажном носителе и актах;
- Полномочия по настоящей доверенности не могут быть переданы третьим лицам.

Подпись лица, получившего доверенность _____ _____

(подпись) (Фамилия И.О.)

Подпись лица, выдавшего доверенность _____ _____

(подпись) (Фамилия И.О.)

УДОСТОВЕРЯЮ

_____ _____ _____

(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

«___» _____ 20__ г.

М.П.

Приложение №3

Форма Заявления на отзыв сертификата ключа подписи

Директору Удостоверяющего центра
ООО «Газинформсервис» Пушкину Н.А.
198188, г. Санкт-Петербург, пр. Стачек, д. 47

От _____
(Должность руководителя)

_____
(Название организации)

_____
(Фамилия И.О. руководителя)

_____
(ИНН/КПП организации)

ЗАЯВЛЕНИЕ

на отзыв сертификата ключа подписи

Прошу Вас аннулировать сертификат ключа подписи сотрудника нашей организации, изготовленный по договору № _____ от «___»_____200__г., и внести аннулированный сертификат ключа подписи в список отозванных сертификатов:

_____
(Должность, Ф.И.О. полностью)

_____
(Причина аннулирования)

Сертификат № _____
(Серийный номер)

_____ _____ _____
(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

«___» _____ 20__ г.

М.П.