Территориальный фонд обязательного медицинского страхования
Самарской области
(ТФОМС Самарской обл.)

УТВЕРЖДАЮ

Директор
Общества с ограниченной
ответственностью по защите
информации «Интерес»
(ООО «Интерес»), г. Тольятти

Р.Р. Богданов

М.П.
«14» августа 2015 г.

УТВЕРЖДАЮ

Директор Территориального
фонда обязательного
медицинского страхования
Самарской области (ТФОМС
Самарской обл.)

В.Н. Мокшин

М.П.
«14» августа 2015 г.

РЕГЛАМЕНТ РАБОТЫ УДОСТОВЕРЯЮЩИЕГО ЦЕНТРА Территориального фонда обязательного медицинского страхования Самарской области

ИС15.003.02.ОРД-УЦ.02.1

Действует с: 14.08.2015

Самара
2015

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Обзорная информация

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего Центра (УЦ) Территориального фонда обязательного медицинского страхования Самарской области (далее по тексту – Владелец УЦ), включая обязанности пользователей (владельцев сертификатов ключей проверки ЭП) и членов группы администрирования УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ.

1.2. Идентификация Регламента

1.2.1. Наименование документа

«Регламент работы Удостоверяющего Центра» Территориального фонда обязательного медицинского страхования Самарской области (шифр: ИС15.003.02.ОРД-УЦ.02.1)

1.2.2. Версия (редакция)

1.0

1.2.3. Дата введения

14.08.2015

1.3. Публикация Регламента

Настоящий Регламент распространяется:

1. В электронной форме:
   1.1. Из репозитария Владельца УЦ по адресу: http://www.samtfoms.ru;
   1.2. Через E-mail от отправителя: general@samtfoms.ru .
   1.3. По защищенному каналу связи VIPNet "Деловая почта" (ViPNet Custom сеть №654)
2. В бумажной форме:
   2.1. Через почтовый адерс: 443082, РФ, Самарская область, г. Самара, ул. Владимирская, д. 60

Копии Регламента, предназначенные для распространения в электронной форме из репозитария Владельца УЦ, распространяются в виде файла, содержащего электронный образ Регламента в формате PDF.

Копии Регламента, предназначенные для распространения в электронной форме через E-mail, распространяются в виде файла, содержащего электронный образ Регламента в формате PDF.

1.4. Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязательства по всем вовлеченным сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.5. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента – 6 лет.

Если Удостоверяющий Центр официально не уведомит пользователей УЦ о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 6 лет.

Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе публикации Регламента.

1.6. Контактная информация

Территориальный фонд обязательного медицинского страхования Самарской области

Почтовый адрес: 443082, РФ, Самарская область, г. Самара, ул. Владимирская, д. 60

Адрес электронной почты: general@samtfoms.ru

Факс: +7(846)339-15-09

1.6.1. Административная Служба УЦ

Контактный телефон: 8 (846) 339-15-25

Адрес электронной почты: Georg@samtfoms.ru

1.6.2. Служба Регистрации УЦ

Контактный телефон: 8 (846) 339-16-33

Адрес электронной почты: sergey.morozov@samtfoms.ru

1.6.3. Служба Безопасности УЦ

Контактный телефон: 8 (846) 339-16-33

Адрес электронной почты: sergey.morozov@samtfoms.ru

1.6.4. Техническая Служба УЦ

Контактный телефон: 8 (846) 339-1525

Адрес электронной почты: Georg@samtfoms.ru

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Назначение Удостоверяющего Центра

Удостоверяющий Центр предназначен для обеспечения участников информационных систем средствами и спецификациями для использования сертификатов ключей проверки электронной подписи в целях обеспечения:

- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- аутентификации участников информационных систем в процессе взаимодействия;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- защищенного обмена электронными документами между пользователями УЦ, в том числе защищенного взаимодействия информационных систем.

2.2. Услуги, предоставляемые Удостоверяющим Центром

В процессе своей деятельности Удостоверяющий Центр предоставляет потребителям (пользователям УЦ) следующие виды услуг:

1. Внесение в реестр Удостоверяющего Центра регистрационной информации о пользователях УЦ;
2. Изготовление сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
3. Формирование ключей электронной подписи и ключей проверки электронной подписи по обращениям пользователей УЦ с записью их на ключевой носитель;
4. Ведение реестра изготовленных сертификатов ключей проверки электронной подписи пользователей УЦ;
5. Предоставление сертификатов ключей проверки электронной подписи в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
6. Аннулирование (отзыв) сертификатов по обращениям владельцев сертификатов ключей проверки электронной подписи;
7. Приостановление и возобновление действия сертификатов по обращениям владельцев сертификатов ключей проверки электронной подписи;
8. Предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах;
9. Подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ;
10. Подтверждение подлинности электронных подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах ключей проверки электронной подписи по обращениям пользователей УЦ;

Иные услуги не предусмотрены.

2.3. Структура Удостоверяющего Центра

Структура УЦ включает в себя следующие организационные подразделения (службы):

- Административная Служба УЦ;
- Служба Регистрации УЦ;
- Служба Безопасности УЦ;
- Техническая Служба УЦ.

2.3.1. Административная служба УЦ

Административная Служба УЦ предназначена для решения задач по:

- управлению деятельностью Удостоверяющего Центра;
- координации деятельности остальных Служб УЦ;
- взаимодействию с пользователями УЦ в части разрешения вопросов, связанных с применением средств ЭП, ключей подписи и сертификатов ключей проверки ЭП, изготовляемых и/или распространяемых Удостоверяющим Центром;
- взаимодействию с пользователями УЦ в части разрешения вопросов, связанных с подтверждением электронной подписи уполномоченного лица Удостоверяющего Центра в сертификатах ключей проверки электронной подписи, изготовленных Удостоверяющим Центром в электронной форме.

2.3.2. Служба Регистрации УЦ

Служба Регистрации УЦ предназначена для решения задач по:

- регистрации пользователей УЦ;
- ведению реестра зарегистрированных пользователей УЦ;
- предоставлению служебных ключей и сертификатов по обращению пользователей УЦ;

Распространение иных средств электронной подписи и шифрования не предусмотрено.

2.3.3. Служба Безопасности УЦ

Служба Безопасности УЦ предназначена для решения задач по:

- организации и выполнению мероприятий по защите ресурсов Удостоверяющего Центра;
- изготовлению и предоставлению ключей по обращению пользователей УЦ;
- изготовлению и предоставлению изготовленных сертификатов ключей проверки ЭП в электронной форме по обращению пользователей УЦ;
- аннулированию (отзыву) сертификатов по обращениям владельцев сертификатов ключей проверки электронной подписи;
- приостановлению и возобновлению действия сертификатов по обращению владельцев сертификатов ключей проверки электронной подписи;

- предоставлению пользователям УЦ сведений об аннулированных и приостановленных сертификатах ключей проверки электронной подписи;
- техническому обеспечению процедуры подтверждения подлинности электронной подписи в документах, представленных в электронной форме, по обращениям пользователей УЦ;
- техническому обеспечению процедуры подтверждения подлинности электронных подписей уполномоченного лица Удостоверяющего центра, в изготовленных сертификатах ключей проверки электронной подписи, по обращениям пользователей УЦ.

2.3.4. Техническая Служба УЦ

Техническая Служба УЦ предназначена для решения задач по:

- организации и выполнению мероприятий по эксплуатации программных и технических средств обеспечения деятельности Удостоверяющего Центра;
- организации и выполнению мероприятий по техническому сопровождению распространяемых средств электронной подписи и шифрования.

2.4. Пользователи услуг Удостоверяющего Центра

Пользователями (потребителями) услуг Удостоверяющего Центра (далее по тексту - пользователи УЦ) называются лица, которые входят в одну или несколько из ниже перечисленных Групп:

Группа 1: пользователи сертификатов ключей проверки ЭП (пользователи, не имеющие собственных сертификатов, но использующие сертификаты других пользователей для каких-либо целей);

Группа 2: зарегистрированные в УЦ лица, являющиеся владельцами пароля для аутентификации в УЦ по паролю;

Группа 3: зарегистрированные в УЦ лица, являющиеся владельцами служебного сертификата ключа проверки ЭП;

Группа 4: зарегистрированные в УЦ лица, являющиеся владельцами рабочих сертификатов ключей проверки ЭП.

Зарегистрированные на УЦ лица, являющиеся владельцами служебных и/или рабочих сертификатов ключей проверки ЭП, все сертификаты которых признаются УЦ недействительными или недействительны по признанию УЦ соответствующие им ключи ЭП, относятся к пользователям Группы 1.

Владельцем сертификата может быть юридическое или физическое лицо.

В случае выдачи сертификата ключа проверки электронной подписи юридическому лицу в качестве владельца сертификата ключа проверки электронной подписи наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Допускается не указывать в качестве владельца сертификата ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в сертификате ключа проверки электронной подписи, используемом для автоматического создания и (или) автоматической проверки электронных подписей.

2.5. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий Центр и пользователь УЦ.

При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

2.6. Платность услуг

Услуга Удостоверяющего Центра по предоставлению сертификатов ключей проверки электронных подписей в электронной форме, находящихся в реестре изготовленных сертификатов, предоставляется на безвозмездной основе.

Примечание:

Состав и стоимость предоставляемых дополнительных услуг определяется Владельцем УЦ.

2.7. Ответственность

Удостоверяющий Центр не несет никакой ответственности в случае нарушения пользователями УЦ положений настоящего Регламента.

Претензии к Удостоверяющему Центру ограничиваются указанием на несоответствие его действий настоящему Регламенту.

2.8. Прекращение деятельности

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

2.9. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент составляется в письменной форме и заверяется собственноручной подписью руководителя Удостоверяющего Центра и печатью Удостоверяющего Центра.

Изменения в Регламент вносятся путем составления дополнительных соглашений к Регламенту, либо заменой Регламента на новую редакцию.

Изменению не подлежат положения настоящего Регламента, прямо или косвенно ущемляющие права пользователей услуг Удостоверяющего Центра.

Утверждение и публикация дополнительных соглашений к Регламенту осуществляется в порядке, соответствующем порядку утверждения и публикации Регламента.

Все изменения и дополнения, вносимые в Регламент в связи с изменением законодательной и нормативной базы, вступают в силу одновременно с вступлением в силу изменений и дополнений в указанных актах. Все остальные изменения вступают в силу и становятся обязательными для Сторон по истечении 10 (десять) календарных дней

с даты размещения указанных изменений и дополнений в Регламенте на сайте http://www.samtfoms.ru ТФОМС Самарской обл. в разделе «Удостоверяющий Центр».

3. ПРАВА СТОРОН

3.1. Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

1. Предоставлять сертификаты ключей проверки ЭП в электронной форме, находящихся в реестре Удостоверяющего Центра, всем лицам, обратившимся в Удостоверяющий Центр;
2. Не проводить регистрацию лиц, обратившихся по вопросу представления сертификатов ключей проверки ЭП в электронной форме, находящихся в реестре Удостоверяющего Центра;
3. Отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
4. Отказать в изготовлении ключей не зарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;
5. Отказать в изготовлении сертификата ключа проверки ЭП зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата, с указанием причин отказа;
6. Отказать в аннулировании (отзыве) сертификата ключа проверки ЭП владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае если истек установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;
7. Отказать в приостановлении или возобновлении действия сертификата ключа проверки ЭП владельцу сертификата, подавшему заявление на приостановление или возобновление действия сертификата, в случае если истек установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;
8. Аннулировать (отозвать) сертификат ключа проверки ЭП пользователя УЦ в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного (отозванного) сертификата и указанием обоснованных причин;
9. Приостановить действие сертификата ключа проверки ЭП пользователя УЦ, с уведомлением владельца приостановленного сертификата ключа проверки ЭП и указанием обоснованных причин.

3.2. Права пользователей УЦ

3.2.1. Пользователи Группы 1

Пользователи сертификатов ключей проверки ЭП (пользователи УЦ, не имеющие собственных сертификатов, но использующие сертификаты других пользователей УЦ для каких-либо целей) имеют следующие права:

1. Получить список аннулированных (отозванных) и приостановленных сертификатов, изготовленный Удостоверяющим Центром;

2. Получить сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра;
3. Получить сертификат ключа проверки ЭП в электронной форме, находящийся в Реестре сертификатов Удостоверяющего Центра;
4. Применять сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра для проверки электронной подписи уполномоченного лица Удостоверяющего Центра в сертификатах, изготовленных Удостоверяющим Центром.
5. Применять сертификаты ключа проверки ЭП в электронной форме для проверки электронной подписи электронного документа.
6. Применять список аннулированных (отозванных) и приостановленных сертификатов, изготовленный Удостоверяющим Центром, для проверки статуса сертификатов ключей проверки ЭП.
7. Обратиться в Удостоверяющий Центр для предоставления им ключа ЭП и ключа проверки ЭП с записью их на ключевой носитель;
8. Обратиться в Удостоверяющий Центр для внесения в реестр Удостоверяющего Центра регистрационной информации о пользователе, с целью в дальнейшем стать владельцем сертификата ключа проверки ЭП;
9. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр запрос на регистрацию в электронной форме;
10. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей в документах, представленных в электронной форме;
11. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах ключей проверки ЭП;
12. Обратиться в Удостоверяющий Центр на предмет получения (приобретения) средства электронной подписи;
13. Сформировать служебные ключи проверки ЭП и ключи ЭП на своем рабочем месте с использованием средства ЭП и программных средств, предоставляемых Удостоверяющим Центром.

3.2.2. Пользователи Группы 2

Зарегистрированные на УЦ лица до положительного результата аутентификации по паролю имеют права пользователей Группы 1.

Зарегистрированные на УЦ лица после положительной аутентификации по паролю имеют права пользователей Группы 1 и дополнительно к ним следующие права:

1. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр запрос в электронной форме на изготовление служебного сертификата ключа проверки ЭП;
2. Обратиться в Удостоверяющий Центр с заявлением в бумажной форме на изготовление служебного сертификата ключа проверки ЭП;
3. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить и установить на свое рабочее место изготовленный служебный сертификат ключа проверки ЭП в электронной форме.

3.2.3. Пользователи Группы 3

Зарегистрированные на УЦ лица до положительного результата аутентификации по служебному сертификату имеют права пользователей Группы 1.

Зарегистрированные на УЦ лица после положительной аутентификации по служебному сертификату имеют права пользователей Группы 1 и дополнительно к ним следующие права:

1. Сформировать рабочие ключи проверки ЭП и ключи ЭП ключи на своем рабочем месте с использованием средства ЭП и программных средств, предоставляемых Удостоверяющим Центром;
2. Обратиться в Удостоверяющий Центр для изготовления рабочего сертификата ключа проверки ЭП;
3. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на изготовление рабочего сертификата ключа проверки ЭП;
4. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить и установить на свое рабочее место изготовленный рабочий сертификат ключа проверки ЭП в электронной форме;
5. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, что бы получить и установить на свое рабочее место изготовленный рабочий сертификат ключа проверки ЭП в электронной форме;
6. Обратиться в Удостоверяющий Центр для аннулирования (отзыва) служебного сертификата ключа проверки ЭП в течение срока действия соответствующего ключа ЭП;
7. Обратиться в Удостоверяющий Центр для приостановления действия служебного сертификата ключа проверки ЭП в течение срока действия соответствующего ключа ЭП;
8. Обратиться в Удостоверяющий Центр для возобновления действия служебного сертификата ключа проверки ЭП в течение срока действия соответствующего ключа ЭП;
9. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на аннулирование (отзыв) служебного сертификата ключа проверки ЭП;
10. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на приостановление действия служебного сертификата ключа проверки ЭП.

3.2.4. Пользователи Группы 4

Зарегистрированные на УЦ лица до положительного результата аутентификации по рабочему сертификату имеют права пользователей Группы 1, а также имеют право применять рабочие ключи ЭП и рабочие сертификаты ключей проверки ЭП, владельцем которых он является, для формирования электронной подписи на электронных документах.

Зарегистрированные на УЦ лица после положительной аутентификации по рабочему сертификату имеют права пользователей Группы 1 и Группы 3, а также дополнительно к ним следующие права:

1. Обратиться в Удостоверяющий Центр для аннулирования (отзыва) рабочего сертификата ключа проверки ЭП в течение срока действия соответствующего ключа ЭП;
2. Обратиться в Удостоверяющий Центр для приостановления действия рабочего сертификата ключа проверки ЭП в течение срока действия соответствующего ключа ЭП;
3. Обратиться в Удостоверяющий Центр для возобновления действия рабочего сертификата ключа проверки ЭП в течение срока действия соответствующего ключа ЭП;
4. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на аннулирование (отзыв) рабочего сертификата ключа проверки ЭП;
5. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на приостановление действия сертификата ключа проверки ЭП;
6. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить по сети сертификаты ключей проверки ЭП в электронной форме из Реестра сертификатов ключей проверки ЭП Удостоверяющего Центра;

4. ОБЯЗАТЕЛЬСТВА СТОРОН

4.1. Обязательства Удостоверяющего Центра

4.1.1. Ключ электронной подписи уполномоченного лица Удостоверяющего Центра

Удостоверяющий Центр обязан использовать для изготовления ключа электронной подписи уполномоченного лица Удостоверяющего Центра и формирования электронной подписи только средства криптографической защиты информации (средства электронной подписи), входящие в состав комплектации ViPNet Custom сеть №654.

Удостоверяющий Центр обязан использовать ключ электронной подписи уполномоченного лица Удостоверяющего Центра только для подписи издаваемых им сертификатов ключей проверки ЭП и списков отозванных сертификатов.

Удостоверяющий Центр обязан принять меры по защите ключа электронной подписи уполномоченного лица Удостоверяющего Центра в соответствии с положениями настоящего Регламента.

4.1.2. Синхронизация времени

Удостоверяющий Центр организует работу своих Служб по Всемирному координированному времени (Universal Time Coordinated - UTC) с учетом часового пояса места расположения Удостоверяющего Центра.

Удостоверяющий Центр обязан синхронизировать по времени все программные и технические средства обеспечения деятельности по предназначению.

4.1.3. Регистрация пользователей УЦ

Удостоверяющий Центр обеспечивает регистрацию пользователей УЦ по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

Удостоверяющий Центр обязан обеспечить уникальность регистрационной информации пользователей УЦ, заносимой в реестр Удостоверяющего Центра и используемой для идентификации владельцев сертификатов ключей проверки ЭП.

Удостоверяющий Центр обязан не разглашать регистрационную информацию пользователей УЦ, за исключением информации, используемой для идентификации владельцев сертификатов ключей проверки ЭП и заносимой в изготавливаемые сертификаты пользователей.

Публикация информации, используемой для идентификации владельцев сертификатов ключей проверки ЭП, осуществляется путем включения ее в изготавливаемые сертификаты.

4.1.4. Изготовление ключей электронной подписи и ключей проверки электронной подписи пользователей УЦ

Удостоверяющий Центр обязан изготовить ключ электронной подписи и ключ проверки ЭП зарегистрированному пользователю по заявлению с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством Российской Федерации.

Удостоверяющий Центр обязан обеспечить сохранение в тайне изготовленного ключа подписи.

Удостоверяющий Центр обязан записать ключ электронной подписи на отчуждаемый носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

Удостоверяющий Центр обязан выполнять процедуру генерации ключей и запись ключей на отчуждаемый носитель только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством Российской Федерации.

4.1.5. Изготовление сертификатов ключей проверки электронной подписи

Удостоверяющий Центр обеспечивает изготовление сертификата ключа проверки ЭП зарегистрированному пользователю по заявлению, в соответствии с форматом и порядком идентификации владельца сертификата, определенным в настоящем Регламенте.

Удостоверяющий Центр обязан обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов пользователей УЦ.

Удостоверяющий Центр обязан обеспечить уникальность значений ключей проверки ЭП в изготовленных сертификатах пользователей УЦ.

4.1.6. Аннулирование (отзыв) сертификатов ключей проверки ЭП

Удостоверяющий Центр обязан аннулировать (отозвать) сертификат ключа проверки ЭП по заявлению его владельца.

Удостоверяющий Центр обязан в течение 24 часов занести сведения об аннулированном (отозванном) сертификате в список отозванных сертификатов с указанием даты и времени занесения и причины отзыва.

4.1.7. Приостановление действия сертификатов ключей проверки ЭП

Удостоверяющий Центр обязан приостановить действие сертификата ключа проверки ЭП по заявлению его владельца.

Удостоверяющий Центр обязан в течение 24 часов занести сведения о приостановленном сертификате в список отозванных сертификатов с указанием даты и времени занесения и признака приостановления.

4.1.8. Возобновление действия сертификатов ключей проверки ЭП

Удостоверяющий Центр обязан возобновить действие сертификат ключа проверки ЭП по заявлению его владельца.

Удостоверяющий Центр обязан в течение 24 часов исключить сведения о приостановленном сертификате из списка отозванных сертификатов.

4.1.9. Уведомления

4.1.9.1. Уведомление о факте изготовления сертификата ключа проверки ЭП

Удостоверяющий Центр обязан официально уведомить о факте изготовления сертификата ключа проверки ЭП его владельца.

Срок уведомления – не позднее 24 часов с момента изготовления сертификата ключа проверки ЭП.

Официальным уведомлением о факте изготовления сертификата является отправка почтового сообщения по электронной почте с прикрепленным сертификатом ключа проверки ЭП в адрес владельца.

Временем отправки почтового сообщения признается время отправки почтового сообщения с почтового сервера, осуществляющего отправку почтовых сообщений Удостоверяющего Центра.

4.1.9.2. Уведомление о факте аннулирования сертификата ключа проверки ЭП

Удостоверяющий Центр обязан официально уведомить о факте аннулирования (отзыва) сертификата ключа проверки ЭП его владельца.

Срок уведомления – не позднее 24 часов с момента занесения сведений об аннулированном (отозванном) сертификате в список отозванных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, в репозитарии Владельца УЦ по адресу http://www.samtfoms.ru.

Временем аннулирования (отзыва) сертификата ключа проверки ЭП признается время занесения сведений об аннулированном (отозванном) сертификате в список отозванных сертификатов, включенное в структуру списка отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается время изготовления списка отозванных сертификатов, включенное в его структуру.

Удостоверяющий Центр обязан включать полный адрес (URL) размещения списка отозванных сертификатов из репозитария Удостоверяющего Центра в издаваемые сертификаты ключей проверки ЭП пользователей УЦ.

4.1.9.3. Уведомление о факте приостановления действия сертификата ключа проверки ЭП

Удостоверяющий Центр обязан официально уведомить о факте приостановления действия сертификата его владельца.

Срок уведомления – не позднее 24 часов с момента занесения сведений о приостановленном сертификате в список отозванных сертификатов.

Официальным уведомлением о факте приостановления действия сертификата является опубликование списка отозванных сертификатов, содержащего сведения о приостановленном сертификате, в репозитарии Владельца УЦ по адресу http://www.samtfoms.ru.

Временем приостановления действия сертификата ключа проверки ЭП признается время занесения сведений о приостановленном сертификате в список отозванных сертификатов, включенное в структуру списка отозванных сертификатов.

Временем опубликование списка отозванных сертификатов признается время изготовления списка отозванных сертификатов, включенное в его структуру.

4.1.9.4. Уведомление о факте возобновления действия сертификата ключа проверки ЭП

Удостоверяющий Центр обязан официально уведомить о факте возобновления действия сертификата его владельца.

Срок уведомления – не позднее 24 часов с момента исключения сведений о приостановленном сертификате из списка отозванных сертификатов.

Официальным уведомлением о факте возобновления действия сертификата является опубликование списка отозванных сертификатов, не содержащем сведения о приостановленном сертификате, в репозитарии Владельца УЦ по адресу http://www.samtfoms.ru. Список отозванных сертификатов должен иметь более позднее, чем приостановление действия сертификата, время изготовления списка отозванных сертификатов, включенное в его структуру.

Временем возобновления действия сертификата ключа проверки ЭП признается время официального уведомления о факте возобновления действия сертификата.

4.1.10. Реестр сертификатов ключей проверки ЭП

Удостоверяющий Центр обязан вести реестр всех изготовленных сертификатов ключей проверки ЭП пользователей УЦ в течение установленного срока хранения.

Реестр сертификатов ключей проверки ЭП ведется в электронном виде.

Удостоверяющий Центр обязан осуществлять предоставление сертификатов ключей проверки ЭП в электронной форме по обращениям пользователей УЦ.

Удостоверяющий Центр обязан публиковать выписки из реестра, позволяющие определить действительность сертификатов ключей проверки пользователей УЦ.

Выписка из реестра Удостоверяющего Центра предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определенном настоящим Регламентом.

4.1.11. Прочие обязательства

Удостоверяющий Центр обязан уведомлять владельца сертификата ключа проверки ЭП о фактах, которые стали известны Удостоверяющему Центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа проверки ЭП.

Удостоверяющий Центр обязан обеспечить передачу пароля от рабочего места пользователя УЦ, проходящего процедуру регистрации в распределенном режиме, посредством защищенного канала связи, реализуемого сертифицированными шифровальными (криптографическими) средствами.

4.2. Обязательства пользователей УЦ

4.2.1. Обязанности лиц, проходящих процедуру регистрации

Лица, проходящие процедуру регистрации в реестре Удостоверяющего Центра, обязаны представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента.

Лица, проходящие процедуру регистрации в распределенном режиме, обязаны хранить в тайне предоставленный пароль для аутентификации по паролю в течение срока действия пароля.

4.2.2. Обязанности владельцев ключей электронной подписи

Владелец ключа электронной подписи обязан:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
- уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена, или заявление на аннулирование (отзыв) которого подано в УЦ;
- использовать для создания и проверки электронных подписей, создания ключей электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

4.2.3. Обязанности пользователей сертификатов ключей проверки ЭП

Перед тем как использовать сертификат ключа проверки ЭП, изготовленный Удостоверяющим Центром, пользователь сертификата (пользователь, не являющийся его владельцем) должен:

- использовать сертификат ключа проверки ЭП только для целей, разрешенных соответствующими областями использования (если такие ограничения указанные в сертификате), определенными в сертификате согласно настоящему Регламенту.

5. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

5.1. Типы конфиденциальной информации

Ключ электронной подписи владельца сертификата ключа проверки ЭП является конфиденциальной информацией данного пользователя УЦ. Удостоверяющий Центр не депонирует и не архивирует ключи электронной подписи пользователей.

Пароль, предоставляемый пользователю УЦ в процессе прохождения процедуры регистрации в распределенном режиме, считается конфиденциальной информацией.

Персональная и корпоративная информация пользователей УЦ, содержащаяся в Удостоверяющем Центре, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки ЭП, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита Удостоверяющего Центра, считается конфиденциальной и не подлежит разглашению.

Отчетные материалы по выполненным проверкам деятельности Удостоверяющего Центра являются конфиденциальными, за исключением заключения по результатам проверок, публикуемого в соответствии с настоящим Регламентом.

5.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

Открытая информация может публиковаться по решению Удостоверяющего Центра. Место, способ и время публикации также определяется решением Удостоверяющего Центра.

Информация, включаемая в сертификаты ключей проверки ЭП пользователей УЦ и списки отозванных сертификатов, издаваемые Удостоверяющим Центром, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

5.3. Исключительные полномочия официальных лиц

Удостоверяющий Центр не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством.

6. ПРОЦЕДУРЫ И МЕХАНИЗМЫ

6.1. Процедура регистрации пользователей УЦ

Под регистрацией пользователей УЦ понимается внесение регистрационной информации о пользователях УЦ в реестр Удостоверяющего Центра.

Процедура регистрации пользователей УЦ применяется в отношении лиц, обращающихся к услугам Удостоверяющего Центра в части изготовления сертификатов

ключей проверки ЭП пользователей УЦ и/или формирования ключей электронной подписи и ключей проверки ЭП пользователей УЦ с записью их на ключевой носитель.

6.1.1. Заявление на регистрацию

Лицо (заявитель), желающее пройти процедуру регистрации в Удостоверяющем Центре, должно подать заявление на регистрацию в Службу Регистрации УЦ (Приложение №1).

Для регистрации лица – будущего владельца сертификата Заявление должно содержать данные, установленные Статьей 17 Федерального закона №63-ФЗ «Об электронной подписи».

К данному заявлению должны прилагаться все необходимые документы, которые подтверждают заносимые в квалифицированный сертификат данные, заверенные печатью заявителя.

Дополнительно (определяется заявителем по согласованию с УЦ) заявление может содержать иную идентифицирующую пользователя информацию.

6.1.2. Идентификация пользователя УЦ

Идентификация пользователя выполняется в процессе его регистрации в качестве зарегистрированного пользователя УЦ.

Результатом идентификации является присвоение пользователю УЦ идентификатора и занесение идентификатора в Реестр зарегистрированных пользователей Удостоверяющего Центра.

Идентификатором зарегистрированного пользователя являются идентификационные данные из заявления на регистрацию (см. раздел 6.1.1 настоящего Регламента).

6.1.3. Регистрация пользователя УЦ в централизованном режиме

Регистрация пользователя УЦ в централизованном режиме осуществляется сотрудником Службы Регистрации УЦ на основе заявления на регистрацию и доверенности на пользователя УЦ (Приложение №3), при личном прибытии ответственного лица, проходящего процедуру регистрации, в офис Удостоверяющего Центра, расположенный по адресу 443082, РФ, Самарская область, г. Самара, ул. Владимирская, д. 60 .

Сотрудник Службы Регистрации УЦ выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по паспорту или иному документу, удостоверяющему личность.

После положительной идентификации лица, проходящего процедуру регистрации, сотрудник Службы Регистрации УЦ принимает бланк заявления на регистрацию.

Бланк заявления на регистрацию должен быть заверен собственноручной подписью заявителя и передан вместе с необходимыми приложениями сотруднику Службы Регистрации УЦ.

Заявление на регистрацию рассматривается Службой Регистрации УЦ в течение от 3 до 10 рабочих дней после поступления заявления.

В случае отказа в регистрации заявление на регистрацию вместе с приложениями возвращается заявителю.

При принятии положительного решения, сотрудник Службы Регистрации УЦ выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего Центра и изготавливает служебные ключи

ЭП и служебный сертификат ключа проверки ЭП (в соответствии с пунктом 7.5 настоящего Регламента).

По окончании процедуры регистрации, зарегистрированному пользователю УЦ выдаются:

- ключи, записанные на ключевой носитель;
- сертификат ключа проверки ЭП в электронной форме, соответствующий ключу ЭП;
- руководство по обеспечению безопасности использования ЭП и средств ЭП;
- сертификаты ключа проверки ЭП уполномоченного лица Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии в электронной форме;
- списки отозванных сертификатов Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии в электронной форме.

Указанные выше данные, передаваемые зарегистрированному пользователю в электронной форме, записываются в виде файлов на сменный носитель (например, флеш-накопитель, usb-токен).

По необходимости (в случае его отсутствия у пользователя), регистрируемый пользователь УЦ должен приобрести (получить) средство электронной подписи, распространяемое дилером данных средств.

С момента подписания обеими сторонами Соглашения о присоединении к Регламенту работы УЦ, заявитель считается присоединившимся к Регламенту и является Стороной Регламента - зарегистрированным Пользователем УЦ.

6.2. Идентификация зарегистрированного пользователя

Идентификация зарегистрированного пользователя УЦ осуществляется по идентификатору зарегистрированного пользователя, занесенному в реестр Удостоверяющего Центра.

6.3. Аутентификация зарегистрированного пользователя

6.3.1. Очная аутентификация зарегистрированного пользователя

Очная аутентификация зарегистрированного пользователя УЦ выполняется по паспорту или другому документу, удостоверяющему личность, предъявляемому лично.

6.3.2. Удаленная аутентификация зарегистрированного пользователя

Удаленная аутентификация зарегистрированного пользователя УЦ предназначена для идентификации зарегистрированного пользователя УЦ по средствам телефонной связи.

Удаленная аутентификация зарегистрированного пользователя УЦ выполняется по ключевой фразе, определенной пользователем в заявлении на регистрацию.

Лицо, проходящее процедуру удаленной аутентификации, должно сообщить свои идентификационные данные и, по запросу сотрудника УЦ, назвать ключевую фразу.

6.3.3. Аутентификация зарегистрированного пользователя по сертификату

Аутентификация зарегистрированного пользователя УЦ по сертификату выполняется путем выполнения процедуры подтверждения электронной подписи с использованием сертификата (в соответствии с пунктом 6.10 настоящего Регламента).

6.4. Изготовление ключей

Изготовление ключей электронной подписи осуществляется Удостоверяющим Центром по обращению граждан. Обращение граждан оформляется в форме заявления на изготовление ключей. Прием заявлений, изготовление и выдача ключей осуществляется Службой Безопасности УЦ при личном присутствии лица, обратившегося с заявлением.

6.4.1. Заявление на изготовление ключей

Заявление на изготовление ключей оформляется заявителем либо по образцу, предоставляемому Службой Безопасности УЦ (Приложение №2).

Заявление на изготовление ключей рассматривается Службой Безопасности УЦ в течение от 3 до 10 рабочих дней с момента поступления.

6.4.2. Изготовление и выдача ключей владельцу

Изготовление ключей выполняется ответственным сотрудником Службы Безопасности УЦ на специализированном рабочем месте, на основании принятого заявления.

Изготовленные ключи записываются на ключевой носитель, предоставляемый заявителем.

Предоставляемый заявителем ключевой носитель должен удовлетворять следующим требованиям:

- иметь тип устройства, входящий в перечень, определяемый Службой Безопасности УЦ;
- быть проинициализированным (отформатированным);
- не содержать никакой информации, за исключением данных инициализации.

Ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой информации не принимаются.

Ключевой носитель, содержащий изготовленные ключи, передается владельцу (заявителю) лично, либо ответственному лицу заявителя по доверенности на получение ключей ЭП (Приложение №4). Факт выдачи ключей заносится в Журнал учета изготовления и выдачи ключей под роспись владельца.

6.5. Изготовление сертификата ключа проверки ЭП и предоставление его владельцу

Изготовление сертификата ключа проверки ЭП осуществляется Удостоверяющим Центром на основании заявления на изготовление сертификата ключа проверки ЭП зарегистрированного пользователя УЦ.

Заявление на изготовление сертификата ключа проверки ЭП подается заявителем в электронной или бумажной форме в Службу Безопасности УЦ.

Заявление на изготовление сертификата в электронной форме подается зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, используемым Удостоверяющим Центром.

Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме подается зарегистрированным пользователем УЦ в офис Службы Безопасности УЦ лично.

Срок рассмотрения заявления на изготовление сертификата ключа проверки ЭП составляет от 3 – 10 рабочих дней с момента его поступления в Службу Безопасности УЦ.

После изготовления сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

Изготовленный сертификат ключа проверки ЭП в электронной форме, заверенный электронной подписью уполномоченного лица Удостоверяющего Центра, предоставляется его владельцу путем отправки с официальным уведомлением в виде прикрепленного файла, содержащего изготовленный сертификат в электронной форме.

6.5.1. Заявление на изготовление сертификата ключа проверки ЭП в электронной форме

Заявление на изготовление сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве подписываемых данных запрос на сертификат в формате PKCS#10 и подписанный электронной подписью с использованием ключа электронной подписи и сертификата ключа проверки ЭП, владельцем которых заявитель является.

В качестве ключа электронной подписи должен использоваться ключ, до окончания срока действия которого, на момент поступления заявления в Службу Безопасности УЦ, остается не менее 1 календарного месяца.

6.5.2. Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме

Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление должно содержать данные, установленные Статьёй 17 63-ФЗ «Об электронной подписи».

К данному заявлению должны прилагаться все необходимые документы, которые подтверждают заносимые в квалифицированный сертификат данные.

Дополнительно (определяется заявителем по согласованию с УЦ) заявление может содержать иную идентифицирующую пользователя информацию.

Заявление должно содержать текст запроса на сертификат в формате PKCS#10 в кодировке Base64.

Обязательным приложением к заявлению на изготовление сертификата в бумажной форме является файл, содержащий запрос на сертификат в формате PKCS#10 в кодировке Base64, размещенный на сменном носителе (например, на флеш-накопителе).

6.5.3. Идентификация владельца сертификата

Владелец сертификата идентифицируется по значениям атрибутов поля Subject сертификата ключа проверки ЭП (см. раздел 8.1 настоящего Регламента).

6.6. Аннулирование (отзыв) сертификата ключа проверки ЭП

Аннулирование (отзыв) сертификата ключа проверки ЭП, изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на отзыв сертификата его владельца (далее по тексту раздела – заявитель).

Заявление на отзыв сертификата ключа проверки ЭП подается заявителем в электронной или бумажной форме в Службу Безопасности УЦ.

Заявление на отзыв сертификата ключа проверки ЭП в электронной форме подается зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, предоставляемого Удостоверяющим Центром.

Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме подается заявителем в офис Службы Безопасности УЦ лично.

Срок рассмотрения заявления на отзыв сертификата ключа проверки ЭП составляет 1 рабочий день с момента его поступления в Службу Безопасности УЦ.

После аннулирования (отзыва) сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

По необходимости отзывается и доверенность на получение ключей ЭП, в этом случае вместе с заявление на аннулирование (отзыв) сертификата ключа проверки ЭП подается заявление на отзыв доверенности (Приложение №6).

6.6.1. Заявление на отзыв сертификата ключа проверки ЭП в электронной форме

Заявление на отзыв сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве подписываемых данных запрос на отзыв сертификата и подписанный электронной подписью с использованием ключа электронной подписи и сертификата ключа проверки ЭП, владельцем которых заявитель является.

Запрос на отзыв сертификата представляет собой строку формата:

```
SN=CertificateSerialNumber,RR=Reason,RC=SomeComment
```

, где:

- CertificateSerialNumber - серийный номер отзываемого сертификата;
- Reason - код причины отзыва из следующего перечня допустимых значений:
  - "0" Не указана
  - "1" Компрометация ключа
  - "2" Компрометация ЦС
  - "3" Изменение принадлежности
  - "4" Сертификат заменен
  - "5" Прекращение работы
- SomeComment - текстовое значение комментария владельца сертификата ключа проверки ЭП.

6.6.2. Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме

Заявление на отзыв сертификата ключа проверки ЭП в бумажной форме (Приложение №5) представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер отзываемого сертификата;
- Причину отзыва сертификата;
- Дата и подпись заявителя.

6.7. Приостановление действия сертификата ключа проверки ЭП

Приостановление действия сертификата ключа проверки ЭП, изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на отзыв сертификата ключа проверки ЭП его владельца (далее по тексту раздела – заявитель).

Заявление на приостановление действия сертификата ключа проверки ЭП подается заявителем в электронной, бумажной или устной форме в Службу Безопасности УЦ.

Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме подается зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, используемым Удостоверяющим Центром.

Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме подается заявителем в офис Службы Безопасности УЦ лично.

Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме подается заявителем в офис Службы Безопасности УЦ по средствам телефонной связи.

Срок рассмотрения заявления на приостановление действия сертификата ключа проверки ЭП составляет 1 рабочий день с момента его поступления в Службу Безопасности УЦ.

После приостановления действия сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

6.7.1. Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме

Заявление на приостановление действия сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве подписываемых данных запрос на приостановление действия сертификата и подписанный электронной подписью с использованием ключа электронной подписи, владельцем которого заявитель является.

Запрос на приостановление действия сертификата представляет собой строку формата:

```
SN=CertificateSerialNumber,RR=Reason,RC=SomeComment,HD=x-x-x-x-x-x
```

, где:

- CertificateSerialNumber - серийный номер сертификата, действие которого приостанавливается;

- Reason – код, имеющий значение "6";
- SomeComment - текстовое значение комментария владельца сертификата, содержащее причину приостановления действия сертификата;
- HD - срок, на который приостанавливается действие сертификата. Срок выражается шестью цифрами, разделенными знаком «-»:
  - позиция 1 – количество лет;
  - позиция 2 – количество месяцев;
  - позиция 3 – количество недель;
  - позиция 4 – количество дней;
  - позиция 5 – количество часов;
  - позиция 6 – количество минут.

6.7.2. Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме

Заявление на приостановление действия сертификата ключа проверки ЭП в бумажной форме (Приложение №7) представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер сертификата, действие которого приостанавливается;
- Срок, на который приостанавливается действие сертификата;
- Причина приостановки действия сертификата;
- Дата и подпись заявителя.

6.7.3. Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме

Заявление на приостановление действия сертификата ключа проверки ЭП в устной форме подается заявителем с прохождением процедуры удаленной аутентификации зарегистрированного пользователя УЦ (см. раздел 6.3.2 настоящего Регламента).

После успешного прохождения процедуры удаленной аутентификации, зарегистрированный пользователь УЦ должен по запросу сотрудника Службы Безопасности УЦ представить следующие сведения:

- Серийный номер сертификата, действие которого приостанавливается;
- Срок, на который приостанавливается действие сертификата;
- Причина приостановки действия сертификата.

6.8. Возобновление действия сертификата ключа проверки ЭП

Возобновление действия сертификата ключа проверки ЭП, изготовленного Удостоверяющим Центром, осуществляется Удостоверяющим Центром по заявлению на возобновление действия сертификата ключа проверки ЭП его владельца (далее по тексту раздела – заявитель).

Заявление на возобновление действия сертификата ключа проверки ЭП подается заявителем в электронной или бумажной форме в Службу Безопасности УЦ.

Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме подается зарегистрированным пользователем УЦ с использованием программного обеспечения зарегистрированного пользователя, предоставляемого Удостоверяющим Центром.

Заявление на возобновление действия сертификата ключа проверки ЭП в бумажной форме подается заявителем в офис Службы Безопасности УЦ лично.

Срок рассмотрения заявления на возобновление действия сертификата ключа проверки ЭП составляет от 3 до 10 рабочих дней с момента его поступления в Службу Безопасности УЦ.

После возобновления действия сертификата ключа проверки ЭП его владельцу направляется официальное уведомление (см. раздел 4.1.9 настоящего Регламента).

6.8.1. Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме

Заявление на возобновление действия сертификата ключа проверки ЭП в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве подписываемых данных запрос на возобновление действия сертификата и подписанный электронной подписью с использованием ключа электронной подписи, владельцем которого заявитель является.

Запрос на возобновление действия сертификата представляет собой строку формата:

```
SN=CertificateSerialNumber,RR=Reason,RC=SomeComment
```

, где:

- CertificateSerialNumber - серийный номер сертификата ключа проверки ЭП, действие которого возобновляется;
- Reason – код, имеющий значение "-1";
- SomeComment - текстовое значение комментария владельца сертификата ключа проверки ЭП, содержащий причину возобновления действия сертификата.

6.8.2. Заявление на возобновление действия сертификата ключа в проверки ЭП в бумажной форме

Заявление на возобновление действия сертификата ключа проверки ЭП в бумажной форме (Приложение №8) представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- Идентификационные данные заявителя;
- Серийный номер сертификата, действие которого возобновляется;
- Причина возобновления действия сертификата;
- Дата и подпись заявителя.

6.9. Срок хранения сертификата ключа проверки ЭП

Хранение сертификата ключа проверки ЭП пользователя УЦ в Реестре сертификатов ключей проверки ЭП осуществляется Удостоверяющим Центром в течение установленного срока действия сертификата ключа проверки ЭП.

Срок архивного хранения сертификата ключа проверки ЭП устанавливается в соответствии со сроком, определенным разделом 7.9 настоящего Регламента.

6.10. Процедура подтверждения электронной подписи с использованием сертификата ключа проверки ЭП

Подтверждение электронной подписи в электронном документе осуществляется Удостоверяющим Центром по обращению граждан (далее по тексту раздела – заявитель), на основании заявления на подтверждение электронной подписи в электронном документе в простой письменной форме (Приложение №10).

Заявление на подтверждение электронной подписи в электронном документе подается заявителем в офис Административной Службы УЦ лично.

Заявление на подтверждение электронной подписи в электронном документе должно содержать информацию от заявителя о дате и времени формирования электронной подписи в электронном документе.

Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя. В качестве доказательства времени подписания электронного документа можете быть предоставлен штамп времени.

Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является магнитный носитель (например, флеш-накопитель), содержащий следующие файлы:

- Файл, содержащий электронный документ, который подписан электронной подписью;
- Файл, содержащий электронную подпись формата PKCS#7 электронного документа, подписанного электронной подписью;
- Файл, содержащий сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра, являющегося издателем сертификата ключа проверки ЭП электронного документа.

Срок рассмотрения заявления на подтверждение электронной подписи в электронном документе составляет от 3 до 10 рабочих дней с момента его поступления в Административную Службу УЦ.

В случае отказа от подтверждения электронной подписи в электронном документе заявителю возвращается заявление на подтверждение электронной подписи в электронном документе с резолюцией ответственного сотрудника Административной Службы УЦ.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи в электронном документе заявителю предоставляется ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Административной Службы УЦ и печатью Удостоверяющего Центра.

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа проверки ЭП принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе;
- отчет по выполненной проверке.

Отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки;
- основания для проведения проверки;
- сведения о членах комиссии, проводившей проверку (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или

ученое звание, занимаемая должность), которой поручено проведение проверки;
- вопросы, поставленные перед комиссией;
- объекты исследований и материалы по заявлению, представленные комиссии для проведения проверки;
- содержание и результаты исследований;
- оценка результатов исследований, выводы по поставленным вопросам;
- иные сведения в соответствии с законодательством РФ.

Отчет составляется в простой письменной форме, заверяется собственноручной подписью членов комиссии и прилагается к заключению.

6.11. Процедура подтверждения электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП

Подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП осуществляется Удостоверяющим Центром по обращению граждан (далее по тексту раздела – заявитель), на основании заявления на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП в простой письменной форме.

Заявление на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП подается заявителем в офис Административной Службы УЦ лично.

Обязательным приложением к заявлению на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП является носитель (например, флеш-накопитель), содержащий следующие файлы:
- Файл, содержащий сертификат ключа проверки ЭП зарегистрированного пользователя УЦ, подвергающийся процедуре проверки;
- Файл, содержащий сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра, являющегося издателем сертификата ключа проверки ЭП пользователя УЦ, подвергающегося процедуре проверки;
- Файл, содержащий список отозванных сертификатов Удостоверяющего Центра, являющегося издателем сертификата ключа проверки ЭП, и использовавшийся для проверки электронной подписи уполномоченного лица Удостоверяющего Центра заявителем.

Срок рассмотрения заявления на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП составляет от 3 до 10 рабочих дней с момента его поступления в Административную Службу УЦ.

В случае отказа от подтверждения электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП заявителю возвращается заявление на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП с резолюцией ответственного сотрудника Административной Службы УЦ.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи уполномоченного лица Удостоверяющего Центра в сертификате ключа проверки ЭП заявителю предоставляется ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Административной Службы УЦ и печатью Удостоверяющего Центра.

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи уполномоченного лица Удостоверяющего Центра на сертификате ключа проверки ЭП и отсутствия искажений в подписанном данной электронной подписью сертификате ключа проверки ЭП пользователя;
- отчет по выполненной проверке.

Отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки;
- основания для проведения проверки;
- сведения о членах комиссии (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки;
- вопросы, поставленные перед комиссией;
- объекты исследований и материалы по заявлению, представленные комиссии для проведения проверки;
- содержание и результаты исследований;
- оценка результатов исследований, выводы по поставленным вопросам;
- иные сведения в соответствии с законодательством.

Отчет составляется в простой письменной форме, заверяется собственноручной подписью членов комиссии и прилагается к заключению.

6.12. Механизм доказательства обладания ключом ЭП, соответствующим сертификату ключа проверки ЭП

Наличие собственноручной подписи владельца сертификата ключа проверки ЭП на документе, содержащем информацию из сертификата (в случае, когда владелец сертификата – физическое лицо), свидетельствует о том, что указанное лицо действительно обладает ключом электронной подписи, соответствующим сертификату ключа проверки электронной подписи, под информацией из которого расписался владелец этого сертификата.

Наличие собственноручной подписи полномочного представителя владельца сертификата ключа проверки ЭП (полномочия которого подтверждаются соответствующей доверенностью) на документе, содержащем информацию из сертификата (в случае, когда владелец сертификата – юридическое лицо), свидетельствует о том, что указанное юридическое лицо действительно обладает ключом электронной подписи, соответствующим сертификату ключа проверки электронной подписи, под информацией из которого расписался полномочный представитель данного юридического лица.

7. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Идентифицирующие данные уполномоченного лица Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра идентифицируется по данным в соответствии с Государственным контрактом, заключенным на сопровождение СКЗИ ТФОМС Самарской обл.

Примечание:

Фамилия, имя и отчество Уполномоченного лица Удостоверяющего центра в сертификат Уполномоченного лица Удостоверяющего центра не заносится.

7.2. Сроки действия ключей уполномоченного лица Удостоверяющего Центра

Максимальный срок действия ключа электронной подписи и сертификата ключа проверки электронной подписи уполномоченного лица УЦ определяется требованиями применяемого в УЦ средства электронной подписи (средства криптографической защиты информации).

Для настоящей редакции применимы сроки:

- Срок действия ключа ЭП уполномоченного лица УЦ – 5 лет;
- Срок действия сертификата ключа проверки ЭП уполномоченного лица УЦ – 15 лет.

Начало периода действия ключа ЭП уполномоченного лица Удостоверяющего Центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП уполномоченного лица УЦ.

7.3. Требования к средствам ЭП, использующимся в составе Удостоверяющего центра и требования к средствам ЭП пользователей УЦ

Средства электронной подписи Удостоверяющего центра должны удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. №796.

Формирование и проверка электронной подписи на серверных компонентах Удостоверяющего центра, а именно на Центре сертификации и Центре регистрации (или Центрах Регистрации, если таковых в Удостоверяющем центре более одного) осуществляется в автоматическом режиме, т.е. электронные подписи на данных компонентах автоматически создаются и автоматически проверяются используемым средством электронной подписи.

На Автоматизированном рабочем месте Администратора Центра регистрации выполнение операции создания электронной подписи осуществляется только после того, как привилегированный пользователь (Администратор, Оператор, Администратор Аудита) ознакомится с содержимым подписываемого документа. После ознакомления - привилегированный пользователь подтверждает создание электронной подписи. Выполнение операции создания электронной подписи заканчивается уведомлением о выполнении операции, связанной с созданием электронной подписи (положительный результат свидетельствует об успешном создании ЭП, отрицательный – ЭП не создана).

На Автоматизированных рабочих местах Администратора Центра регистрации и разбора конфликтных ситуаций выполнение операции проверки электронной подписи сопровождается ознакомлением с электронным документом, информированием о внесении изменений в электронный документ (при изменении электронного документа появляется сообщение – электронная подпись – «Не верна»), отображением сертификата ключа проверки ЭП подписчика данного электронного документа.

Для формирования электронной подписи, средства электронной подписи пользователя Удостоверяющего центра средства электронной подписи Удостоверяющего центра должны удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. №796.

7.4. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП пользователей УЦ

Максимальный срок действия ключа ЭП пользователя УЦ, соответствующего сертификату ключа проверки ЭП, владельцем которого он является, определяется требованиями средства электронной подписи (средства криптографической защиты информации), использующим данный ключ ЭП.

Начало периода действия ключа ЭП пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП пользователя УЦ.

Максимальный срок действия сертификата ключа проверки ЭП пользователя УЦ определяется требованиями средства электронной подписи (средства криптографической защиты информации), использующим ключ ЭП пользователя, соответствующий указанному сертификату.

Конкретный срок действия сертификата ключа проверки ЭП пользователя устанавливается Удостоверяющим Центром при его изготовлении.

Срок действия сертификата ключа проверки ЭП пользователя УЦ определяется путем выбора минимального из установленных сроков областей использования сертификатов, приведенных в Таблице 7.1, из числа областей использования, указанных в соответствующем заявлении на изготовление сертификата ключа проверки ЭП.

Таблица 7.1. Таблица сроков областей использования сертификатов

№ п/п	Наименование области использования	Срок
1	**2**	**3**
1	Центр Регистрации	5 лет
2	Администратор Центра Регистрации	5 лет
3	Оператор Центра Регистрации	1 год
4	Пользователь Центра Регистрации	1 год
5	Временный доступ к Центру Регистрации	1 неделя
6	Защищенная электронная почта	1 год
7	Проверка подлинности клиента	1 год
8	Проверка подлинности сервера	1 год

7.5. Служебные ключи ЭП и служебный сертификат ключа проверки ЭП

Служебные ключи ЭП и служебный сертификат ключа проверки ЭП предназначены только для:

- обеспечения аутентификации зарегистрированного пользователя УЦ при использовании программного обеспечения зарегистрированного пользователя УЦ, предоставляемого Удостоверяющим Центром;
- формирования электронной подписи в заявлении на сертификат ключа проверки ЭП в электронном виде.

Служебный сертификат ключа проверки ЭП содержит следующие области использования:

- Проверка подлинности клиента;
- Пользователь Центра Регистрации;
- Временный доступ к Центру Регистрации.

Срок действия служебного ключа ЭП устанавливается равным сроку действия соответствующего служебного сертификата ключа проверки ЭП.

Срок действия служебного сертификата ключа проверки ЭП устанавливается равным сроку, соответствующему области использования «Временный доступ к Центру Регистрации» из Таблица 7.1.

7.6. Рабочие ключи ЭП и рабочий сертификат ключа проверки ЭП

Рабочие ключи ЭП и рабочий сертификат ключа проверки ЭП предназначены для:

- обеспечения аутентификации и авторизации зарегистрированного пользователя УЦ при использовании программного обеспечения зарегистрированного пользователя УЦ, предоставляемого Удостоверяющим Центром;
- формирования электронной подписи в заявлении на рабочий сертификат (последующий) ключа проверки ЭП в электронном виде;
- формирования электронной подписи электронных документов.

7.7. Меры защиты ключей ЭП

Ключи ЭП пользователей УЦ должны записываться при их генерации на типы ключевых носителей, которые поддерживаются используемым средством ЭП.

Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство ЭП.

Если процедуру генерации ключей пользователя УЦ выполняет сотрудник Удостоверяющего Центра, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключа ЭП.

Ответственность за конфиденциальность сохранение пароля (ПИН-кода) возлагается на владельца ключа ЭП.

Сотрудники Удостоверяющего Центра, являющиеся владельцами ключей ЭП, также выполняют указанные в настоящем разделе меры защиты ключей ЭП.

7.8. Информация из сертификата ключа проверки ЭП на бумажном носителе

При получении сертификата заявителем он должен быть под расписку ознакомлен Удостоверяющим Центром с информацией, содержащейся в сертификате.

При оформлении данной расписки в бумажной форме указанная информация должна включать сведения установленные Статьей 17 Федерального закона №63-ФЗ «Об электронной подписи.

7.9. Архивное хранение документированной информации

7.9.1. Состав документов, подлежащих архивному хранению

Архивированию подлежит следующая документированная информация:

- Реестр сертификатов ключей проверки ЭП пользователей УЦ;
- сертификаты ключей проверки ЭП уполномоченного лица Удостоверяющего Центра;
- журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего Центра;
- Реестр зарегистрированных пользователей Удостоверяющего Центра;

- заявления на изготовление сертификатов ключей проверки ЭП пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов ключей проверки ЭП;
- заявления на приостановление действия сертификатов ключей проверки ЭП;
- заявления на возобновление действия сертификатов ключей проверки ЭП:
- служебные документы Удостоверяющего Центра.

7.9.2. Источник комплектования архивного фонда

Источником комплектования архивного фонда Удостоверяющего Центра являются подразделения (Службы) Удостоверяющего Центра, обеспечивающие документирование.

7.9.3. Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

7.9.4. Срок архивного хранения

Документы Удостоверяющего центра, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов устанавливается 5 лет.

7.9.5. Уничтожение архивных документов

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

7.10. Смена ключей уполномоченного лица Удостоверяющего Центра

7.10.1. Плановая смена ключей уполномоченного лица Удостоверяющего Центра

Плановая смена ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) уполномоченного лица Удостоверяющего Центра должна выполняться в течение срока действия ключа ЭП уполномоченного лица УЦ.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего Центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего Центра формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- Уполномоченное лицо Удостоверяющего Центра изготавливает новый сертификат ключа проверки ЭП на новом ключе ЭП Уполномоченного лица Удостоверяющего центра.

Старый ключ ЭП уполномоченного лица Удостоверяющего Центра используется в течении своего срока действия для формирования списков

отозванных сертификатов в электронной форме, изданных Удостоверяющим Центром в период действия старого ключа ЭП уполномоченного лица Удостоверяющего Центра.

7.10.2. Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа ЭП уполномоченного лица Удостоверяющего Центра.

Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего Центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего Центра.

8. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

8.1. Структура сертификата ключа проверки ЭП, изготавливаемого Удостоверяющим Центром в электронной форме

Удостоверяющий Центр издает сертификаты ключей проверки ЭП пользователей УЦ и уполномоченного лица Удостоверяющего Центра в электронной форме X.509 версии 3.

Структура квалифицированного сертификата ключа проверки ЭП должна удовлетворять требованиям Приказа ФСБ России от 27.12.2011 г. №795 «Об утверждении требований у форме квалифицированного сертификата ключа проверки электронной подписи».

8.2. Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме

Удостоверяющий Центр издает списки отозванных сертификатов ключей проверки ЭП в электронной форме (далее по тексту раздела – СОС) формата X.509 версии 2.

Таблица 8.1. Структура списка отозванных сертификатов

Название	Описание	Содержание
1	**2**	**3**
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра в соответствии с Приказом ФСБ России от 27.12.2011 г. №795
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата

1	2	3
		(CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа ЭП уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего центра
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС

9. ПРОГРАММНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для реализации своих услуг и обеспечения деятельности Удостоверяющий Центр использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра (далее по тексту – ПК УЦ);
- Технические средства обеспечения работы ПК УЦ (далее по тексту – ТС УЦ);
- Программные и программно-аппаратные средства защиты информации (далее по тексту – СЗИ УЦ);

9.1. Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра

Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра включает в себя следующие программные компоненты:

1. Центр Сертификации;
2. Центр Регистрации;
3. АРМ администратора ЦР;
4. АРМ разбора конфликтных ситуаций.

Центр Сертификации является базовым серверным компонентом ПК УЦ и предназначен для обеспечения реализации следующих целевых функций Удостоверяющего Центра:

1. Формирования сертификатов ключей проверки ЭП пользователей УЦ в электронной форме с использованием ключа ЭП и сертификата ключа проверки ЭП уполномоченного лица Удостоверяющего Центра;
2. Формирования списков аннулированных (отозванных) и приостановленных сертификатов пользователей УЦ (СОС) в электронной форме с использованием ключа ЭП и сертификата ключа проверки ЭП уполномоченного лица Удостоверяющего Центра;
3. Ведения эталонной копии Реестра сертификатов ключей проверки ЭП Удостоверяющего Центра;
4. Ведения реестра изданных списков аннулированных (отозванных) и приостановленных сертификатов ключей проверки ЭП пользователей УЦ;
5. Обеспечения уникальности ключей проверки ЭП в изданных сертификатах ключей проверки ЭП пользователей УЦ.

Ответственность за эксплуатацию Центра Сертификации возлагается на уполномоченное лицо Удостоверяющего Центра.

Центр Регистрации является серверным компонентом ПК УЦ и предназначен для обеспечения реализации следующих целевых функций Удостоверяющего Центра:

1. Ведения Реестра зарегистрированных пользователей Удостоверяющего Центра;
2. Ведения Реестра сертификатов ключей проверки ЭП Удостоверяющего Центра;
3. Ведения Реестра заявлений на изготовление сертификатов пользователей УЦ в электронной форме;
4. Ведения Реестра заявлений на аннулирование (отзыв) сертификатов пользователей УЦ в электронной форме;
5. Ведения Реестра заявлений на приостановление действия сертификатов пользователей УЦ в электронной форме;
6. Ведения Реестра запросов на регистрацию пользователей УЦ в электронной форме;
7. Ведения Реестра заявлений на возобновление действия сертификатов пользователей УЦ в электронной форме;
8. Предоставления программных средств для:
   8.1. Пользователей УЦ Группы 1 для обеспечения реализации их права передать по сети на Удостоверяющий Центр запрос на регистрацию в электронной форме;
   8.2. Зарегистрированных пользователей УЦ Группы 2 и 3 для обеспечения реализации их прав в части пользования предоставляемыми программными средствами;

Ответственность за эксплуатацию Центра Регистрации возлагается на Службу Регистрации УЦ.

АРМ администратора ЦР является приложением ПК УЦ и предназначен для обеспечения реализации своих функциональных обязанностей сотрудникам Службы Регистрации и Службы Безопасности УЦ.

АРМ разбора конфликтных ситуаций является приложением ПК УЦ и предназначен для обеспечения своих функциональных обязанностей сотрудникам Административной Службы УЦ в части взаимодействия с пользователями УЦ при разрешении вопросов, связанных с подтверждением электронной подписи

уполномоченного лица Удостоверяющего Центра в сертификатах ключей проверки ЭП, изготовленных Удостоверяющим Центром в электронной форме.

9.2. Технические средства обеспечения работы ПК УЦ

Технические средства обеспечения работы ПК УЦ включают в себя:

- Выделенный сервер Центра Сертификации;
- Выделенный сервер Центра Регистрации;
- Телекоммуникационное оборудование;
- Компьютеры рабочих мест сотрудников Служб Удостоверяющего Центра;
- Устройства печати на бумажных носителях (принтеры).

Ответственность за эксплуатацию технических средств и общесистемного программного обеспечения возлагается на Техническую Службу УЦ.

9.3. Программные и программно-аппаратные средства защиты информации

Программные и программно-аппаратные средства защиты информации включают в себя:

- Средства криптографической защиты информации (средства электронной подписи);
- Межсетевой экран для обеспечения защиты компонент УЦ при сетевом взаимодействии;
- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Устройства обеспечения бесперебойного питания серверов Центра Сертификации и Центра Регистрации;
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений Удостоверяющего Центра;
- Устройства обеспечения противопожарной безопасности помещений Удостоверяющего Центра.

На компонентах Удостоверяющего центра должны использоваться средства криптографической защиты информации (средства электронной подписи), входящие в состав комплектации ViPNet Custom сеть №654.

Ответственность за эксплуатацию программных и программно-аппаратных средств защиты информации возлагается на Техническую Службу УЦ.

9.4. Перечень событий, регистрируемых программным комплексом обеспечения деятельности Удостоверяющего Центра

- Центром Сертификации:
  - Установлено сетевое соединение с программной компонентой Центра Регистрации;
  - Издан СОС;
  - Принят запрос на сертификат;
  - Издание сертификата;
  - Невыполнение внутренней операции программной компоненты;

- Системные события общесистемного программного обеспечения.

– Центром Регистрации:
  - Помещен запрос на регистрацию;
  - Принят запрос на регистрацию;
  - Отклонен запрос на регистрацию;
  - Помещен запрос на сертификат;
  - Принят запрос на сертификат;
  - Отклонен запрос на сертификат;
  - Установка сертификата подтверждена пользователем;
  - Помещен запрос на отзыв сертификата;
  - Принят запрос на отзыв сертификата;
  - Отклонен запрос на отзыв сертификата;
  - Помещен запрос на первый сертификат;
  - Запрошен список отозванных сертификатов;
  - Опубликован список отозванных сертификатов;
  - Невыполнение внутренней операции программной компоненты;
  - Установлено сетевое соединение с внешней программной компонентой;
  - Системные события общесистемного программного обеспечения.

Структуры записей событий приведены в эксплуатационной документации ПК УЦ и общесистемного программного обеспечения.

9.5. Перечень данных программного комплекса обеспечения деятельности Удостоверяющего Центра, подлежащих резервному копированию

При эксплуатации программного комплекса обеспечения деятельности Удостоверяющего Центра ежесуточно выполняется резервное копирование данных компонент ПК УЦ.

Перечень данных ПК УЦ, подлежащих резервному копированию, включает в себя:

– Сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра в электронном виде (сертификат службы сертификации Центра Сертификации ПК УЦ);
– Базу данных службы сертификации Центра Сертификации ПК УЦ, включая журнал выданных сертификатов и очередь запросов;
– Базу данных Центра Регистрации ПК УЦ (базу данных SQL сервера Центра Регистрации);
– Журналы аудита компонент ПК УЦ в составе, определенном эксплуатационной документацией ПК УЦ.

10. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

10.1. Инженерно-технические меры защиты информации

10.1.1. Размещение технических средств Удостоверяющего Центра

Сервера Центра Сертификации, Центра Регистрации и телекоммуникационное оборудование должны быть размещены в серверном помещении.

Сервера Центра Сертификации, Центра Регистрации и телекоммуникационное оборудование размещаются в шкафу-стойке (сервеная).

Остальные технические средства Удостоверяющего Центра размещаются в рабочих помещения Удостоверяющего Центра по схеме организации рабочих мест персонала.

10.1.2. Физический доступ в помещения

Серверное помещение Удостоверяющего Центра оборудовано системой контроля доступа (идентификация при пропуске сотрудника в здание Организации через систему СКУД, передача опечатанного тубуса с ключами на вскрытие серверной и пломбы (штампа) на опечатывание серверной, при вскрытии помещения – идентификация по звонку ответственного лица при прохождении объемного датчика движения).

Серверное помещение оборудовано исполнительным устройством системы контроля доступа механического типа.

Рабочие и служебные помещения Удостоверяющего Центра не подключены к системе контроля доступа и оборудованы механическими замками.

Идентификационные карты для доступа в серверное помещение выдаются сотрудникам из состава Службы Безопасности и Технической Службы УЦ по приказу руководителя Удостоверяющего Центра.

Ключи механических замков рабочих помещений Удостоверяющего Центра выдаются сотрудникам Удостоверяющего Центра по распоряжению руководителя Административной Службы УЦ на основании схемы организации рабочих мест персонала.

10.1.3. Электроснабжение и кондиционирование воздуха

Технические средства Удостоверяющего Центра подключены к общегородской сети электроснабжения.

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».

Сервера Центра Сертификации и Центра Регистрации, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение не менее 1 часа после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников Удостоверяющего Центра, источниками бесперебойного питания не оборудуются.

Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Служебные помещения Удостоверяющего Центра, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения Удостоверяющего Центра оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

10.1.4. Подверженность воздействию влаги

Защита серверов Центра Сертификации и Центра Регистрации и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке (сервеная).

10.1.5. Предупреждение и защита от возгорания

Серверное помещение Удостоверяющего Центра оборудовано пожарной сигнализации.

Пожарная безопасность помещений Удостоверяющего Центра обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

10.1.6. Хранение документированной информации

Документальный фонд Удостоверяющего Центра, как фондообразователя, подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

10.1.7. Уничтожение документированной информации

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

10.2. Программно-аппаратные меры защиты информации

10.2.1. Организация доступа к техническим средствам Удостоверяющего Центра

Доступ к техническим средствам Удостоверяющего Центра, размещенным в серверном помещении, осуществляется с использованием системы контроля доступа.

Организация доступа к техническим средствам Удостоверяющего Центра, размещенных на рабочих местах сотрудников Удостоверяющего Центра, возлагается на сотрудников Удостоверяющего Центра, ответственных за эксплуатацию данных технических средств.

10.2.2. Организация доступа к программным средствам Удостоверяющего Центра

Сервера Центра Сертификации и Центра Регистрации оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок», SecretNet.

Рабочие места сотрудников Удостоверяющего Центра, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» оснащены сертифицированными программным комплексами защиты от несанкционированного доступа типа SecretNet.

Устройство типа «Электронный замок» при локальной аутентификации администраторов на технических компонентах удостоверяющего центра должно ограничивать количество подряд следующих неудачных попыток доступа числом не более 3.

Доступ системных администраторов общесистемного программного обеспечения серверов Центра Сертификации и Центра Регистрации для выполнения регламентных работ осуществляется в присутствии сотрудников Службы Безопасности УЦ, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения (Центра Сертификации и/или Центра Регистрации).

10.2.2.1. Общий перечень объектов доступа УЦ

К объектам доступа Удостоверяющего центра относятся:
- технические средства компонент УЦ;
- программное обеспечение компонент УЦ: ПО Центра сертификации, ПО Центра регистрации, ПО АРМ администратора Центра регистрации, ПО АРМ разбора конфликтных ситуаций, ПО, предназначенное для регистрации и управления сертификатами пользователей УЦ;
- базы данных компонент УЦ: база данных ЦС, база данных ЦР;
- ключи ЭП и сертификаты ключей проверки ЭП;
- списки отозванных сертификатов УЦ.

10.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам Удостоверяющего центра

Сотрудникам Административной Службы УЦ:
- технические средства Центра сертификации и Центра регистрации УЦ;
- технические средства АРМ разбора конфликтных ситуаций;
- программное обеспечение Центра сертификации и Центра регистрации УЦ;
- база данных Центра сертификации и Центра регистрации УЦ;
- ключи и сертификаты, использующиеся для эксплуатации Центра сертификации и Центра регистрации;
- списки отозванных сертификатов УЦ.

Сотрудникам Службы Регистрации УЦ:
- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные ключи ЭП и сертификаты ключей проверки ЭП сотрудников Службы Регистрации;
- служебные ключи ЭП и служебные сертификаты ключей проверки ЭП пользователей УЦ;
- рабочие сертификаты ключей проверки ЭП пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам Службы Безопасности УЦ:
- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные ключи ЭП и сертификаты ключей проверки ЭП сотрудников Службы Безопасности;

- служебные сертификаты ключей проверки ЭП пользователей УЦ;
- рабочие ключи и рабочие сертификаты ключей проверки ЭП пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам Технической службы УЦ:
- технические средства компонент УЦ;
- программное обеспечение компонент УЦ;
- базы данных Центра сертификации и Центра регистрации.

10.2.2.3.Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами Удостоверяющего Центра

Пользователям УЦ Группы 1:
- программное обеспечение формирования запроса на регистрацию пользователя УЦ;

Пользователям УЦ Группы 2:
- программное обеспечение формирования служебных ключей и запроса на служебный сертификат аутентифицированного пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изданного служебного сертификата аутентифицированного пользователя УЦ;
- личные служебные ключи ЭП и служебные сертификаты ключей проверки ЭП.

Пользователям УЦ Группы 3:
- сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра в электронной форме;
- список аннулированных (отозванных) сертификатов ключей проверки в электронной форме;
- программное обеспечение предоставления учетной информации о сертификатах аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение предоставления учетной информации о запросах (заявлениях) в электронной форме, поступивших на Удостоверяющий Центр от аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение формирования рабочих ключей и заявления на рабочий сертификат ключа проверки ЭП в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изданного рабочего сертификата ключа проверки ЭП аутентифицированного пользователя УЦ;
- программное обеспечение формирования заявления на аннулирование (отзыв) служебного сертификата в электронной форме аутентифицированного пользователя УЦ;

- программное обеспечение формирования заявления на приостановление действия служебного сертификата в электронной форме аутентифицированного пользователя УЦ;
- личные рабочие ключи ЭП и рабочие сертификаты ключей проверки ЭП.

Пользователям УЦ Группы 4:

- сертификат ключа проверки ЭП уполномоченного лица Удостоверяющего Центра в электронной форме;
- список аннулированных (отозванных) сертификатов ключей проверки ЭП в электронной форме;
- сертификаты ключей проверки ЭП пользователей Удостоверяющего Центра в электронной форме;
- программное обеспечение предоставления учетной информации о сертификатах аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение предоставления учетной информации о запросах (заявлениях) в электронной форме, поступивших на Удостоверяющий Центр от аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение формирования рабочих ключей и заявления на рабочий сертификат ключа проверки ЭП в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изданного рабочего сертификата ключа проверки ЭП аутентифицированного пользователя УЦ;
- программное обеспечение формирования заявления на аннулирование (отзыв) служебного сертификата в электронной форме аутентифицированного пользователя УЦ
- программное обеспечение формирования заявления на приостановление действия служебного сертификата в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение формирования заявления на возобновление действия служебного сертификата в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение предоставления учетной информации о сертификатах ключей проверки ЭП пользователей УЦ в электронной форме.
- личные рабочие ключи и рабочие сертификаты ключей проверки ЭП.

10.2.3. Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого Удостоверяющим Центром:

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Центра Сертификации;
- Программные модули Центра Регистрации;
- Программные модули АРМ администратора ЦР;
- Программные модули АРМ разбора конфликтных ситуаций.

Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом Удостоверяющего Центра, утверждаемый руководителем Удостоверяющего Центра.

Система контроля целостности программных модулей, подлежащих контролю целостности, основывается на аппаратном контроле целостности и общесистемного программного обеспечения до загрузки операционной системы.

Данная система контроля целостности обеспечивается использованием сертифицированного устройства типа «электронный замок».

Контроль целостности программных модулей средств электронной подписи и средств криптографической защиты информации осуществляется средствами электронной подписи и средствами криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности – ежесуточно.

Ответственность за выполнение мероприятий по контролю целостности программных средств возложена на Службу Безопасности УЦ.

10.2.4. Контроль целостности технических средств

Контроль целостности технических средств технических средств Удостоверяющего Центра обеспечивается опечатыванием корпусов устройств, препятствующим их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию и после выполнения регламентных работ.

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

Ответственность за выполнение мероприятий по контролю целостности технических средств возложена на Службу Безопасности УЦ.

10.2.5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности Удостоверяющего Центра и программными средствами, предоставляемыми Удостоверяющим Центром пользователям УЦ, в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации.

Защита программно-технических средств обеспечения деятельности Удостоверяющего Центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана сертифицированного ФСБ России не ниже 4-го класса защиты.

10.2.5.1. Перечень информации, подлежащей защите

Поступающая в Удостоверяющий Центр информация:

- Заявление на регистрацию в электронной форме;
- Заявление на изготовление сертификата в электронной форме;
- Заявление на аннулирование (отзыв) сертификата в электронной форме;
- Заявление на приостановление действия сертификата в электронной форме;
- Заявление на возобновление действия сертификата в электронной форме;

- Пароль, передаваемый пользователем УЦ при аутентификации по паролю;
- Ключевая фраза пользователя УЦ.

Передаваемая из Удостоверяющего Центра информация:
- Пароль, передаваемый пользователю УЦ для аутентификации по паролю;
- Список сертификатов пользователя УЦ и их статус;
- Список запросов на сертификаты пользователя УЦ и их статус;
- Список запросов на аннулирование (отзыв), приостановление и возобновление действия сертификатов пользователя УЦ и их статус.

10.3. Организационные меры защиты информации

10.3.1. Предъявляемые требования к персоналу Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более двух лет.

Сотрудники Службы Безопасности УЦ имеют высшее профессиональное образование и прошли курсы повышения квалификации в области информационной безопасности с получением специализации в области систем с открытым распределением ключей.

10.3.2. Профессиональная переподготовка и повышение квалификации персонала

Профессиональная переподготовка персонала Удостоверяющего Центра не осуществляется.

Сотрудники Удостоверяющего Центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в два года.

10.3.3. Организация сменной работы

Деятельность Удостоверяющего Центра по работе с пользователями УЦ в части приема заявлений в бумажной форме и изготовления сертификатов ключей проверки ЭП организована в одну рабочую смену с 9.00 до 18.00 в рабочие дни согласно законодательства Российской Федерации.

10.3.4. Организация доступа персонала к документам и документации

Доступ сотрудников Удостоверяющего Центра к документам и документации, составляющей документальный фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

10.3.5. Охрана здания и помещений

Удостоверяющий Центр имеет собственную (и/или привлекаемую) службу охраны здания и помещений, обеспечивающую:
- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) Удостоверяющего Центра;

- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

10.4. Юридические меры защиты информации

Удостоверяющий Центр имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг.

Системы безопасности Удостоверяющего Центра и защиты информации созданы и поддерживаются на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством Российской Федерации.

Все меры по защите информации на Удостоверяющем Центре введены в действие приказами руководителя Удостоверяющего Центра.

Для обеспечения деятельности Удостоверяющий Центр использует средства электронной подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы Удостоверяющего Центра находятся в собственности Удостоверяющего Центра.

11. ПРИЛОЖЕНИЯ

Приложение А. Сокращения
Приложение Б. Термины и определения
Приложение В. Структуры записей аудита
Приложение Г. Руководство по обеспечению безопасности ЭП

1. Форма Заявления на присоединение к Регламенту УЦ
2. Форма Заявления на изготовление ключей (сертификата ключа подписи)
3. Форма Доверенности Пользователя УЦ
4. Форма Доверенности на получение ключей
5. Форма Заявления на аннулирование (отзыв) сертификатов ключей проверки ЭП
6. Форма Заявления на отзыв доверенности
7. Форма Заявления на приостановление действия сертификата ключа проверки ЭП
8. Форма Заявления на возобновление действия сертификата ключа проверки ЭП
9. Форма Заявления на получение информации о статусе сертификата ключа подписи, изданного УЦ
10. Форма Заявления на подтверждение подлинности электронной подписи в электронном документе (с резолюцией)

ПРИЛОЖЕНИЕ А
к Регламенту работы
Удостоверяющего Центра

СОКРАЩЕНИЯ

БД	–	база данных
ПАК	–	программно-аппаратный комплекс;
ПК	–	программный комплекс;
РФ	–	Российская Федерация;
СКЗИ	–	средство криптографической защиты информации;
СОС	–	список отозванных сертификатов;
ФЗ	–	Федеральный закон;
ФСБ	–	Федеральная служба безопасности;
УЦ	–	удостоверяющий центр;
ЦР	–	центр регистрации;
ЦС	–	центр сертификации;
ЭД	–	электронный документооборот;
ЭП	–	электронная подпись.

ПРИЛОЖЕНИЕ Б
к Регламенту работы
Удостоверяющего Центра

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аккредитация удостоверяющего центра
Признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона.

Аутентификация
Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности электронной подписи.

Запрос на сертификат
Сообщение, содержащее необходимую информацию для получения сертификата.

Запрос на отзыв сертификата
Сообщение, содержащее необходимую информацию для отзыва сертификата.

Идентификация
Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)
Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

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

Ключ электронной подписи
Уникальная последовательность символов, предназначенная для создания ЭП.

Ключевой носитель
Носитель, предназначенный для хранения и содержащий ключ электронной подписи и/или дополнительную служебную информацию.

Компрометация ключа
Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Плановая смена ключей
Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи

Список отозванных сертификатов

Созданный УЦ список сертификатов, отозванных до окончания срока их действия.

Средства электронной подписи

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

Средства удостоверяющего центра

Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Удостоверяющий центр

Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

Центр сертификации

Компонент удостоверяющего центра. Выполняет функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

Центр регистрации

Компонент удостоверяющего центра. Выполняет функции промежуточного звена, осуществляющего передачу запросов от пользователей и администраторов центра регистрации центру сертификации.

Электронная подпись

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

ПРИЛОЖЕНИЕ В

СТРУКТУРЫ ЗАПИСЕЙ АУДИТА

Таблица В1. Структура записи аудита модуля политики службы сертификации ЦС

Поле	Описание
1	**2**
Время	Дата и время, разделенные пробелом, когда произошло данное событие
Событие	Код типа данного события
ID запроса	Идентификатор запроса на сертификат
Subject запроса	Группа значений, разделенная запятыми, определяющая субъекта запроса
Usage запроса	Группа значений, разделенная запятыми, определяющая области использования запрашиваемого сертификата в запросе
Subject сертификата	Группа значений, разделенная запятыми, определяющая субъекта (владельца) сертификата
Usage сертификата	Группа значений, разделенная запятыми, определяющая области использования сертификата
Serial сертификата	Серийный (регистрационный) номер сертификата
FileName COC	Имя файла, содержащего сформированный список отозванных сертификатов (CRL)

Дополнительная информация при детализации события, располагается после поля Событие, зависит от типа события и содержит группу полей. Поля, не заполняемые при детализации события, заполняются пустым значением.

Все поля в записи журнала аудита разделяются знаком табуляции.

Таблица В2. Структура записи аудита ПО Центра Регистрации

Поле	Описание
1	**2**
EventID	Уникальный идентификатор данного события
EventTypeID	Идентификатор типа данного события, определенного в таблице EventType
EventDate	Дата, когда произошло данное событие
EventDescripton	Текстовое описание данного события
UserID	Идентификатор пользователя, который выполнил задачу, породившую данное событие, и определенного в таблице UserInfo1
SubjectID	Идентификатор пользователя, являющегося субъектом, для которого выполнялась задача, породившая данное событие, и определенного в таблице UserInfo1

Таблица В3. Структура записи аудита Windows 2008 Server

Поле	Описание
1	**2**
Дата	Дата, когда произошло данное событие.
Время	Локальное время, когда произошло данное событие.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода.
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера.
Код события	Число, определяющее конкретный тип события. В первой строке описания

1	2
	обычно содержится название типа события. Например, 6005 — это идентификатор события, которое происходит при запуске службы ведения журналов событий. Соответственно, в начале описания этого события находится строка «Запущена служба журнала событий». Код события и имя источника записи могут использоваться представителями группы поддержки программного продукта для устранения неполадок.
Источник	Программа, занесшая событие. Это может быть как имя программы (например, «SQL Server»), так и название компонента системы или большого приложения (например, название драйвера). Например, «Elnkii» означает драйвер EtherLink II.
Тип	Уровень важности события: «Ошибка», «Уведомление» или «Предупреждение» в журналах системы и приложений; «Аудит успехов» или «Аудит отказов» в журнале безопасности. В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория события в зависимости от источника события. Это сведения используются преимущественно в журнале безопасности. Например, для аудита событий безопасности категория соответствует одному из типов событий, для которых в групповой политике может быть включен аудит успехов или отказов.

Таблица В4. Структура записи аудита MS Internet Information Server (IIS)

Поле	Обозначение в журнале аудита	Описание
1	**2**	**3**
Дата	date	Дата возникновения события.
Время	time	Время возникновения события.
IP-адрес клиента	c-ip	IP-адрес клиента, получившего доступ к серверу.
Имя пользователя	c-username	Имя пользователя, получившего доступ к серверу. Это не относится к анонимным пользователям, которые обозначаются черточками.
Имя службы	s-sitename	Служба Интернета, выполнявшаяся на компьютере клиента, и номер экземпляра.
Имя сервера	s-computername	Имя сервера, на котором была создана запись журнала.
Адрес IP сервера	s-ip	IP-адрес сервера, на котором была создана запись журнала.
Метод	cs-method	Действие, которое пытался выполнить клиент (например, метод GET).
Ресурс URI	cs-uri-stem	Ресурс, к которому было выполнено обращение, например Default.htm.
Запрос URI	cs-uri-query	Запрос, который пытался выполнить клиент.
Состояние протокола	sc-status	Состояние действия (в терминах HTTP).
Состояние Win32	sc-win32-status	Состояние действия.
Передано байт	sc-bytes	Число байт, отправленных сервером.
Получено байт	cs-bytes	Число байт, полученных сервером.
Порт сервера	s-port	Номер порта, к которому подключен клиент.
Заняло времени	time-taken	Время, которое заняло выполнение действия.
Версия протокола	cs-protocol	Версия протокола (HTTP, FTP), используемого клиентом. Для протокола HTTP это либо HTTP 1.0, либо HTTP 1.1.
Агент пользователя	cs(User-Agent)	Обозреватель, используемый клиентом.
Объект Cookie	cs(Cookie)	Содержимое отправленного или полученного модуля настройки клиента (cookie) (если имеется).
Источник ссылки	cs(Referer)	Предыдущий просмотренный пользователем узел. На этом узле содержалась ссылка на данный узел.

Все поля в записи журнала аудита разделяются пробелами.

Таблица В5. Структура записи аудита SQL Server

Поле	Описание
1	**2**
Дата	Дата возникновения события.
Время	Время возникновения события.
Процесс	Имя серверного процесса
Описание	Текстовое описание события

Все поля в записи журнала аудита разделяются пробелами.

ПРИЛОЖЕНИЕ Г
к Регламенту работы
Удостоверяющего Центра

РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЭП

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи:
   1.1. Обеспечить конфиденциальность ключей электронных подписей.
   1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.
   1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
   1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.
   1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
   1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
   1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.
   1.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.
   1.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
2. Порядок применения средств квалифицированной электронной подписи:
   2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.