РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ

Общества с ограниченной ответственностью «Удостоверяющий центр ГАЗИНФОРМСЕРВИС»

Утвержден приказом №28 от 15 мая 2012 года

Редакция 2.1

Санкт-Петербург

2013 г.

Оглавление

1. ВВЕДЕНИЕ 9
1.1. Обзор 9
1.2. Наименование и идентификация документа 9
1.3. Участники 9
1.3.1. Удостоверяющий центр 9
1.3.2. Центр регистрации 9
1.3.3. Владелец сертификата ключа проверки электронной подписи 9
1.3.4. Пользователь сертификата ключа проверки электронной подписи 9
1.3.5. Другие участники 10
1.4. Использование сертификатов ключей проверки электронных подписей 10
1.4.1. Допустимое использование сертификата ключа проверки электронной подписи 10
1.4.2. Недопустимое использование сертификата ключа проверки электронной подписи 10
1.5. Управление документом 10
1.5.1. Организация, ответственная за содержание документа 10
1.5.2. Контактное лицо 10
1.5.3. Лица, утверждающие изменения 10
1.5.4. Процедура утверждения изменений 10
1.6. Определения и сокращения 10
2. ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ 11
2.1. Реестр выданных сертификатов 11
2.2. Публикация реестра выданных сертификатов 11
2.3. Время и частота публикаций реестра 11
2.4. Доступ к реестру 11
3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ 12
3.1. Имена (наименования) 12
3.1.1. Типы имен 12
3.1.2. Необходимость в значимых именах (наименованиях) 12

3.1.3. Правила интерпретации различных форм имен (наименований) 12
3.1.4. Уникальность имен (наименований) 12
3.1.5. Использование торговых марок 12
3.2. Процедура первичной регистрации 12
3.2.1. Способ доказательства факта владения ключом электронной подписи 12
3.2.2. Процедура аутентификации юридического лица 12
3.2.3. Процедура аутентификации индивидуального предпринимателя 13
3.2.4. Процедура аутентификации физического лица 13
3.2.5. Сведения, указанные в заявлении, не подвергающиеся проверке 13
3.2.6. Дополнительные условия аутентификации 13
3.2.7. Подтверждение полномочий владельца сертификата ключа проверки электронной подписи 14
3.2.8. Взаимодействие с владельцами сертификатов ключей проверки электронных подписей, выданными другими удостоверяющими центрами 14
3.3. Идентификация и аутентификация заявителя при смене ключей 14
3.3.1. Идентификация и аутентификация в случае плановой (очередной) смены ключей 14
3.3.2. Идентификация и аутентификация в случае смены ключей после отзыва (аннулирования) 14
3.3.3. Идентификация и аутентификация заявителя при подаче заявления на отзыв (аннулирование) сертификата 14
4. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА 14
4.1. Заявление на выдачу сертификата ключа подписи 14
4.1.1. Лица, имеющие право подавать заявления на выпуск сертификатов ключей проверки электронных подписей 15
4.1.2. Процедура регистрации и обязательства 15
4.1.3. Форма заявления на выдачу сертификата ключа проверки электронной подписи 16
4.2. Обработка заявления на выдачу сертификата ключа проверки электронной подписи 16
4.2.1. Процедура идентификации и аутентификации 16
4.2.2. Выдача и отказ в выдаче сертификата ключа проверки электронной подписи 16
4.2.3. Сроки рассмотрения заявления на выдачу сертификата ключа проверки электронной подписи 16
4.3. Изготовление сертификата ключа проверки электронной подписи 16

4.3.1. Действия удостоверяющего центра при изготовлении сертификата ключа проверки электронной подписи 16

4.3.2. Уведомление заявителя о факте изготовления сертификата ключа проверки электронной подписи 16

4.4. Акцепт (признание) сертификата 16

4.4.1. Действия владельца сертификата ключа проверки электронной подписи, означающие акцепт сертификата 16

4.4.2. Публикация сертификата 16

4.4.3. Уведомление пользователей удостоверяющего центра о выдаче сертификата ключа проверки электронной подписи 16

4.5. Использование ключей и сертификатов ключей проверки электронной подписи 17

4.5.1. Использование ключа электронной подписи и сертификата ключа проверки электронной подписи их владельцем 17

4.5.2. Использование ключа проверки электронной и сертификата ключа проверки электронной подписи пользователем 17

4.6. Обновление сертификата ключа проверки электронной подписи 17

4.7. Смена ключей 17

4.8. Изменение сведений, указанных в сертификате ключа проверки электронной подписи 17

4.9. Отзыв и приостановление действия сертификата проверки электронной подписи 17

4.9.1. Условия отзыва сертификата 18

4.9.2. Лица, уполномоченные подавать заявления на отзыв сертификатов ключей проверки электронных подписей 18

4.9.3. Процедура подачи заявления на отзыв сертификата ключа проверки электронной подписи 18

4.9.4. Форма заявления на отзыв сертификата ключа проверки электронной подписи 18

4.9.5. Срок подачи заявления на отзыв сертификата ключа проверки электронной подписи 18

4.9.6. Срок обработки заявления на отзыв сертификата ключа проверки электронной подписи 18

4.9.7. Требования к осуществлению проверки факта отзыва сертификата ключа проверки электронной подписи 18

4.9.8. Частота выпуска списков отозванных сертификатов 18

4.9.9. Задержка публикации списков отозванных сертификатов 19

4.9.10. Возможность онлайновой проверки статуса сертификата 19

4.9.11. Требования к осуществлению онлайновой проверки факта отзыва сертификата 19

4.9.12. Другие способы извещения участников информационных систем о фактах отзыва сертификатов 19
4.9.13. Особые требования в случае компрометации ключей 19
4.9.14. Условия приостановления действия сертификата 19
4.9.15. Лица, уполномоченные подавать заявления на приостановление действия сертификата 19
4.9.16. Процедура подачи заявления на приостановление действия сертификата 19
4.9.17. Ограничение срока приостановления действия сертификата 20
4.10. Сервис онлайновой проверки статуса сертификата 20
4.10.1. Рабочие характеристики 20
4.10.2. Доступность службы проверки статусов сертификатов 20
4.10.3. Дополнительные возможности 20
4.11. Окончание пользования услугами удостоверяющего центра 20
4.12. Депонирование и восстановление ключей 20
5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ 20
5.1. Физические меры обеспечения безопасности 20
5.1.1. Здания и сооружения 20
5.1.2. Физический доступ 20
5.1.3. Электроснабжение и кондиционирование воздуха 21
5.1.4. Подверженность воздействию влаги 21
5.1.5. Предупреждение и защита от возгорания 21
5.1.6. Хранение архивных документов и электронных носителей 21
5.1.7. Уничтожение документированной информации 21
5.1.8. Резервная площадка 21
5.2. Организационные меры обеспечения безопасности 22
5.2.1. Разграничение ролей (полномочий) 22
5.3. Требования к персоналу 23
5.3.1. Квалификации персонала 23
5.3.2. Проверка биографии сотрудников 23
5.3.3. Требования к повышению квалификации персонала 23

5.3.4. Требования к повторному прохождению обучения 23
5.3.5. Частота и последовательность смены деятельности сотрудников 23
5.3.6. Ответственности за нарушения 23
5.3.7. Требования к независимым подрядчикам 23
5.3.8. Документационное обеспечение персонала 23
5.4. Порядок ведения записей аудита 23
5.4.1. Типы событий, подлежащих аудиту 23
5.4.2. Частота анализа журналов аудита 24
5.4.3. Срок хранения журналов аудита 24
5.4.4. Защита журналов аудита 24
5.4.5. Резервное копирование журналов аудита 24
5.4.6. Условия сбора записей аудита 24
5.4.7. Уведомление субъекта события, вносимого в журнал аудита. 24
5.4.8. Анализ уязвимостей 24
5.5. Ведение архива 24
5.5.1. Типы архивных записей 24
5.5.2. Срок хранения архива 24
5.5.3. Защита архива 24
5.5.4. Резервное копирование архива 24
5.5.5. Требования к простановке времени создания архивных записей 25
5.5.6. Условия архивирования 25
5.5.7. Порядок получения и проверки информации, хранящейся в архиве 25
5.6. Смена ключей УЦ 25
5.7. Восстановление в случае компрометации или аварии 25
5.7.1. Действия по предотвращению компрометации и аварии 25
5.7.2. Случаи повреждения оборудования, программных и/или аппаратных сбоев 25
5.7.3. Компрометация ключа участника информационной системы 25
5.7.4. Восстановление работоспособности после аварии 26
5.8. Разрешение конфликтных ситуаций 26

5.8.1. Некорректность входящего электронного документа или электронной подписи 26

5.8.2. Непризнание отправителем электронного документа факта отправки документа, а также его целостности и подлинности 27

Процедура проверки ЭП документа 27

5.9. Прекращение работы удостоверяющего центра 28

6. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ 28

6.1. Изготовление и установка ключевой пары 28

6.1.1. Изготовление ключей 28

6.1.2. Передача ключа электронной подписи владельцу 28

6.1.3. Передача ключа проверки электронной подписи в удостоверяющий центр 28

6.1.4. Передача ключей проверки электронных подписей участникам информационных систем 28

6.1.5. Размеры ключей 28

6.1.6. Параметры генерации и проверки качества ключа электронной подписи 29

6.1.7. Цели использования ключа (порядок заполнения поля key usage сертификата x.509v3) 29

6.2. Защита ключа электронной подписи, требования к ключевым носителям и криптографическим модулям 29

6.2.1. Требования к ключевым носителям 29

6.2.2. Ключ электронной подписи, контролируемый несколькими держателями (n из m) 29

6.2.3. Депонирование ключа электронной подписи 29

6.2.4. Резервное копирование ключа электронной подписи 29

6.2.5. Архивирование ключа электронной подписи 29

6.2.6. Запись ключа электронной подписи в криптографический модуль (ключевой носитель) 30

6.2.7. Хранение ключа электронной подписи в криптографическом модуле (ключевом носителе) 30

6.2.8. Способы активации ключа электронной подписи 30

6.2.9. Способы деактивации ключа электронной подписи 30

6.2.10. Способы уничтожения ключа электронной подписи 30

6.2.11. Оценка криптографического модуля (ключевого носителя) 30

6.3. Другие особенности использования ключей электронной подписи 30

6.3.1. Архивирование ключей проверки электронных подписей 30

6.3.2. Сроки действия сертификатов и ключей 30
6.4. Данные активации ключей электронных подписей 31
6.4.1. Генерация и установка данных активации ключа электронной подписи 31
6.4.2. Защита данных активации ключа электронной подписи 31
6.4.3. Особенности данных активации ключа электронной подписи 31
6.5. Меры обеспечения информационной безопасности 31
7. ПРОФИЛИ СЕРТИФИКАТОВ И CRL 31
7.1. Профиль сертификата 31
7.1.1. Версия сертификата 32
7.1.2. Расширения сертификата 32
7.1.3. Объектные идентификаторы алгоритмов 32
7.1.4. Форматы имен (идентификационных данных) 33
7.1.5. Ограничения, накладываемые на имена (идентификационные данные) 34
7.1.6. Объектный идентификатор политики сертификата 34
7.1.7. Использование расширения Policy Constraints 34
7.1.8. Использование расширения Policy Qualifier 34
7.1.9. Порядок обработки расширений Certificate Policies, имеющих пометку critical. 34
7.2. Профиль CRL 34
7.3. Дополнения CRL 34

1. ВВЕДЕНИЕ

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

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

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

1.1. Обзор

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

1.2. Наименование и идентификация документа

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

Объектный идентификатор: 1.2.643.3.190.1.1-2.1

Версия документа: 2.1

Дата: 18.05.2012 с изменениями от 30 мая 2013 г.

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

1.3. Участники

1.3.1. Удостоверяющий центр

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ от 06 апреля 2011 года.

1.3.2. Центр регистрации

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

1.3.3. Владелец сертификата ключа проверки электронной подписи

Владелец сертификата ключа проверки электронной подписи – лицо, которому в порядке, установленном Федеральным законом № 63-ФЗ от 06 апреля 2011 года, выдан сертификат ключа проверки электронной подписи.

1.3.4. Пользователь сертификата ключа проверки электронной подписи

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

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

1.3.5. Другие участники

Уполномоченный федеральный орган исполнительной власти в сфере использования электронной подписи, осуществляющий ведение Единого государственного реестра квалифицированных сертификатов ключей проверки электронных подписей удостоверяющих центров в соответствии с действующим законодательством РФ.

1.4. Использование сертификатов ключей проверки электронных подписей

1.4.1. Допустимое использование сертификата ключа проверки электронной подписи

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

1.4.2. Недопустимое использование сертификата ключа проверки электронной подписи

Сертификаты ключей проверки электронных подписей, выдаваемые ООО «УЦ ГИС» не должны использоваться для формирования электронной подписи и шифрования сведений составляющих государственную тайну.

1.5. Управление документом

1.5.1. Организация, ответственная за содержание документа

ООО «УЦ ГИС»
198097, Россия, Санкт-Петербург, пр. Стачек, 47.

1.5.2. Контактное лицо

Заместитель генерального директора ООО «УЦ ГИС»
198188, Россия, Санкт-Петербург, пр. Стачек, а/я 63.
+7 (812) 3-052-052
ca@gaz-is.ru

1.5.3. Лица, утверждающие изменения

Изменения регламента утверждаются руководителем удостоверяющего центра.

1.5.4. Процедура утверждения изменений

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

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

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

1.6. Определения и сокращения

Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом[1].

Сертификат ключа проверки электронной подписи(ЭП) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и

[1] Федеральный закон «Об электронной подписи» №63-ФЗ от 06.004.2011 г.

подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи[2].

Квалифицированный сертификат ключа проверки электронной подписи (далее - 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

COC – список отозванных (аннулированных) сертификатов.

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

TSP – time stamping protocol, протокол меток времени.

2. ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1. Реестр выданных сертификатов

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

2.2. Публикация реестра выданных сертификатов

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

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

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

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

2.3. Время и частота публикаций реестра

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

Сведения о статусе сертификатов публикуются в соответствии с настоящим регламентом.

2.4. Доступ к реестру

[2] Федеральный закон «Об электронной подписи» №63-ФЗ от 06.004.2011 г.

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

Удостоверяющий центр осуществляет защиту от несанкционированного доступа к реестру.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. Имена (наименования)

3.1.1. Типы имен

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

3.1.2. Необходимость в значимых именах (наименованиях)

Указанные в сертификатах ключей проверки электронных подписей Ф.И.О. физических лиц точно совпадают со сведениями, указанными в предъявленных государственных документах, удостоверяющих личность.

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

3.1.3. Правила интерпретации различных форм имен (наименований)

Нет условий.

3.1.4. Уникальность имен (наименований)

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

3.1.5. Использование торговых марок

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

3.2. Процедура первичной регистрации

3.2.1. Способ доказательства факта владения ключом электронной подписи

Заявитель должен продемонстрировать факт обладания ключом электронной подписи, соответствующим ключу проверки электронной подписи, который указан в заявлении и будет указан в сертификате. Способом доказательства владения ключом электронной подписи является электронный документ формате PKCS#10.

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

3.2.2. Процедура аутентификации юридического лица

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

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

2. Дополнительные подтверждающие документы в случаях, указанных в п. 2. ст.18 Федерального закона «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ.

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

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

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

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

- устав с изменениями – нотариально заверенные копии;

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

3.2.3. Процедура аутентификации индивидуального предпринимателя

Если заявление подается от имени индивидуального предпринимателя, заявитель предоставляет:

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

2. Дополнительные подтверждающие документы в случаях, указанных в п. 2. ст.18 Федерального закона «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ.

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

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

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

3.2.4. Процедура аутентификации физического лица

При подаче заявления от физического лица, заявитель предоставляет:

1. Страховое свидетельство обязательного пенсионного страхования (СНИЛС);
2. Паспорт или другой государственный документ, удостоверяющий личность;
3. Дополнительные подтверждающие документы в случаях, указанных в п. 2. ст.18 Федерального закона «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ.

3.2.5. Сведения, указанные в заявлении, не подвергающиеся проверке

Нет условий.

3.2.6. Дополнительные условия аутентификации

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

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

В случае подачи заявления законным представителем заявителя, законный представитель должен представить доверенность от заявителя на осуществление действий от его имени. Образец доверенности доступен по ссылке: http://ca.gaz-is.ru/repository/onbehalfform.cagis.doc.

3.2.7. Подтверждение полномочий владельца сертификата ключа проверки электронной подписи

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

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

Владельцы сертификатов ключей проверки электронных подписей удостоверяющего центра ООО «УЦ ГИС» могут быть участниками единого пространства доверия с владельцами сертификатов ключей проверки электронных подписей выданными другими удостоверяющими центрами в тех случаях, когда:
- между удостоверяющими центрами заключено соответствующее соглашение и приняты необходимые организационно-технические меры;
- владелец сертификата ключа проверки электронной подписи, выданного удостоверяющим центром ООО «УЦ ГИС» является пользователем сертификата ключа проверки электронной подписи, выданного другим удостоверяющим центром.

3.3. Идентификация и аутентификация заявителя при смене ключей

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

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

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

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

Процедура проводится в порядке, описанном в п. 3.2.

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

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

4. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1. Заявление на выдачу сертификата ключа подписи

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

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

4.1.2. Процедура регистрации и обязательства

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

Процедура регистрации владельца сертификата ключа проверки электронной подписи применяется в отношении физических лиц (в т. ч. представляющих интересы юридических лиц), обращающихся к услугам удостоверяющего центра в части изготовления сертификатов ключей подписей и/или изготовления ключей электронной подписи и ключей проверки электронной подписи с записью их на ключевой носитель.

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

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

Заявления, поданные от физического лица, должны обязательно содержать следующие сведения:
- фамилию, имя и отчество;
- страховой номер индивидуального лицевого счета (СНИЛС);
- реквизиты основного документа, удостоверяющего личность;
- адрес электронной почты;
- контактные телефоны.

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

Удостоверяющий центр вправе требовать от заявителя предоставления дополнительных сведений, определенных регламентами и актами владельцев информационных систем, в которых будет использоваться электронная подпись заявителя.

4.1.3. Форма заявления на выдачу сертификата ключа проверки электронной подписи

Форма заявления на выдачу сертификата ключа проверки электронной подписи доступна по ссылке: http://ca.gaz-is.ru/repository/appform.cagis.doc.

4.2. Обработка заявления на выдачу сертификата ключа проверки электронной подписи

4.2.1. Процедура идентификации и аутентификации

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

4.2.2. Выдача и отказ в выдаче сертификата ключа проверки электронной подписи

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

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

4.2.3. Сроки рассмотрения заявления на выдачу сертификата ключа проверки электронной подписи

Удостоверяющий центр обрабатывает заявления в коммерчески оправданные сроки. Как правило, срок обработки заявления не превышает одного рабочего дня. Время выдачи сертификата, как правило, не превышает 45 минут.

4.3. Изготовление сертификата ключа проверки электронной подписи

4.3.1. Действия удостоверяющего центра при изготовлении сертификата ключа проверки электронной подписи

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

4.3.2. Уведомление заявителя о факте изготовления сертификата ключа проверки электронной подписи

Сертификат ключа проверки электронной подписи передается владельцу в электронном виде путем установки в ключевой контейнер, на съемном носителе или по адресу электронной почты, указанному в сертификате и публикуется в реестре на интернет-сайте удостоверяющего центра.

4.4. Акцепт (признание) сертификата

4.4.1. Действия владельца сертификата ключа проверки электронной подписи, означающие акцепт сертификата

Следующие действия владельца сертификата ключа проверки электронной подписи означают акцепт сертификата:
- загрузка файла сертификата или его установка из полученного электронного документа;
- неполучение удостоверяющим центром мотивированных возражений (претензий) по поводу содержания сертификата ключа проверки электронной подписи в течение 5 рабочих дней с даты выдачи сертификата.

4.4.2. Публикация сертификата

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

4.4.3. Уведомление пользователей удостоверяющего центра о выдаче сертификата ключа проверки электронной подписи

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

4.5. Использование ключей и сертификатов ключей проверки электронной подписи

4.5.1. Использование ключа электронной подписи и сертификата ключа проверки электронной подписи их владельцем

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

4.5.2. Использование ключа проверки электронной и сертификата ключа проверки электронной подписи пользователем

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

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

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

4.6. Обновление сертификата ключа проверки электронной подписи

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

В настоящее время указанная процедура не производится.

4.7. Смена ключей

Смена ключей – процедура выдачи нового сертификата ключа проверки электронной подписи. Данная процедура подразумевает изготовление новых ключей электронной подписи и проверки электронной подписи.

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

4.8. Изменение сведений, указанных в сертификате ключа проверки электронной подписи

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

4.9. Отзыв и приостановление действия сертификата проверки электронной подписи

4.9.1. Условия отзыва сертификата

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

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

Заявление на отзыв сертификата ключа проверки электронной подписи может подавать только его владелец, удостоверяющие центры и центры регистрации, участвовавшие в процессе обработки заявлений на выдачу этих сертификатов.

4.9.3. Процедура подачи заявления на отзыв сертификата ключа проверки электронной подписи

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

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

4.9.4. Форма заявления на отзыв сертификата ключа проверки электронной подписи

Форма заявления на отзыв сертификата ключа подписи доступна по ссылке: http://ca.gaz-is.ru/repository/revokeform.cagis.doc.

4.9.5. Срок подачи заявления на отзыв сертификата ключа проверки электронной подписи

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

4.9.6. Срок обработки заявления на отзыв сертификата ключа проверки электронной подписи

Удостоверяющий центр в течение одного рабочего дня заносит информацию об отозванном сертификате в список отозванных сертификатов и публикует его на интернет-сайте удостоверяющего центра.

4.9.7. Требования к осуществлению проверки факта отзыва сертификата ключа проверки электронной подписи

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

4.9.8. Частота выпуска списков отозванных сертификатов

Списки отозванных сертификатов публикуются не реже одного раза в сутки.

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

4.9.9. Задержка публикации списков отозванных сертификатов

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

4.9.10. Возможность онлайновой проверки статуса сертификата

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

4.9.11. Требования к осуществлению онлайновой проверки факта отзыва сертификата

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

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

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

Нет условий.

4.9.13. Особые требования в случае компрометации ключей

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

4.9.14. Условия приостановления действия сертификата

Удостоверяющий центр может приостановить действие сертификата ключа проверки электронной подписи и осуществить публикацию его в списке отозванных сертификатов в следующих случаях:

- получение от владельца сертификата ключа проверки электронной подписи заявления на приостановление действия сертификата;

- удостоверяющий центр имеет доказательства нарушения владельцем сертификата условий настоящего регламента и/или условий договора об оказании услуг или обязательств перед другими участниками информационных систем.

4.9.15. Лица, уполномоченные подавать заявления на приостановление действия сертификата

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

4.9.16. Процедура подачи заявления на приостановление действия сертификата

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

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

4.9.17. Ограничение срока приостановления действия сертификата

Срок, на который приостанавливается действия сертификата, не может быть больше срока действия сертификата, оставшегося с момента подачи заявления до окончания срока его действия.

4.10. Сервис онлайновой проверки статуса сертификата

4.10.1. Рабочие характеристики

Сервис онлайновой проверки статуса сертификата реализует протокол OCSP поверх HTTP в соответствии с RFC 2560 «X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP» с использованием российских криптографических алгоритмов.

Производительность сервиса: до 3700 ответов/сек.

4.10.2. Доступность службы проверки статусов сертификатов

Информация о статусах сертификатов доступна постоянно за исключением запланированных перерывов в работе.

4.10.3. Дополнительные возможности

Нет условий.

4.11. Окончание пользования услугами удостоверяющего центра

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

4.12. Депонирование и восстановление ключей

Удостоверяющий центр не осуществляет депонирования и восстановления ключей.

5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

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

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

Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты от несанкционированного доступа. Этот контроль выполняется администраторами безопасности не реже 1 раза в месяц.

5.1. Физические меры обеспечения безопасности

5.1.1. Здания и сооружения

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

5.1.2. Физический доступ

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

Серверное оборудование размещается в центрах обработки данных и серверных помещениях, соответствующих требованиям действующего законодательства, предъявляемым к обеспечению безопасности удостоверяющих центров.

Помещения удостоверяющего центра круглосуточно находятся под охраной специализированной организации.

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

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

5.1.3. Электроснабжение и кондиционирование воздуха

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

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

Помещения удостоверяющего центра оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

5.1.4. Подверженность воздействию влаги

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

5.1.5. Предупреждение и защита от возгорания

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

5.1.6. Хранение архивных документов и электронных носителей

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

5.1.7. Уничтожение документированной информации

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

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

5.1.8. Резервная площадка

Нет условий.

5.2. Организационные меры обеспечения безопасности

5.2.1. Разграничение ролей (полномочий)

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

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

Оператор УЦ осуществляет:
- регистрацию заявлений;
- ведение реестра абонентов;
- распространение средств ЭП;
- изготовление криптографических ключей;
- изготовление и предоставление изготовленных сертификатов ключей проверки электронных подписей в электронной форме по обращению участников информационных систем;
- изготовление и предоставление сертификатов ключей проверки электронных подписей на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) сертификатов ключей проверки электронных подписей по обращениям их владельцев;
- предоставление участникам информационных систем сведений об аннулированных сертификатах ключей проверки электронных подписей;
- предоставление участникам информационных систем сертификатов ключей проверки электронных подписей, находящихся в реестре изготовленных сертификатов;
- техническое обеспечение процедуры подтверждения электронной подписи в документах, представленных в электронной форме, по обращениям участников информационных систем;
- техническое обеспечение процедуры подтверждения подлинности электронной подписи уполномоченного лица удостоверяющего центра, в изготовленных сертификатах ключей проверки электронных подписей, по обращениям участников информационных систем.

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

Аудитор осуществляет внутренний аудит деятельности УЦ. проверку журналов регистрации событий общесистемного, прикладного и специализированного программного обеспечения, а также проводит периодический контроль защищенности программно-технических средств УЦ.

5.3. Требования к персоналу

5.3.1. Квалификации персонала

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

5.3.2. Проверка биографии сотрудников

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

5.3.3. Требования к повышению квалификации персонала

Сотрудники удостоверяющего центра проходят курсы повышения квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 5 лет.

5.3.4. Требования к повторному прохождению обучения

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

5.3.5. Частота и последовательность смены деятельности сотрудников

Нет условий.

5.3.6. Ответственности за нарушения

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

5.3.7. Требования к независимым подрядчикам

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

5.3.8. Документационное обеспечение персонала

Деятельность сотрудников удостоверяющего центра регламентирована внутренними инструкциями удостоверяющего центра.

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

5.4. Порядок ведения записей аудита

5.4.1. Типы событий, подлежащих аудиту

Программно-аппаратный комплекс УЦ регистрирует следующие виды событий:

- системные события общесистемного программного обеспечения;
- помещение запроса на сертификат проверки электронной подписи;
- принятие запроса на сертификат проверки электронной подписи;
- выпуск сертификата ключа проверки электронной подписи;
- отклонение запроса на сертификат проверки электронной подписи;
- выпуск списка отозванных сертификатов проверки электронной подписи;
- невыполнение внутренней операции программной компоненты.

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

5.4.2. Частота анализа журналов аудита

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

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

5.4.3. Срок хранения журналов аудита

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

5.4.4. Защита журналов аудита

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

5.4.5. Резервное копирование журналов аудита

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

5.4.6. Условия сбора записей аудита

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

5.4.7. Уведомление субъекта события, вносимого в журнал аудита.

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

5.4.8. Анализ уязвимостей

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

5.5. Ведение архива

5.5.1. Типы архивных записей

Удостоверяющий центр ведет архив:

- журналов аудита в соответствии с п.5.4;
- соглашений с владельцами сертификатов ключей проверки электронных подписей, договоров;
- заявлений на выдачу и отзыв сертификатов ключей проверки электронных подписей.

5.5.2. Срок хранения архива

Удостоверяющий центр хранит архив на протяжении всего срока работы.

5.5.3. Защита архива

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

5.5.4. Резервное копирование архива

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

5.5.5. Требования к простановке времени создания архивных записей

Нет условий.

5.5.6. Условия архивирования

Удостоверяющий центр обеспечивает ведение архива в соответствии с законодательством РФ.

5.5.7. Порядок получения и проверки информации, хранящейся в архиве

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

5.6. Смена ключей УЦ

Заблаговременно до окончания срока действия ключа электронной подписи уполномоченного лица удостоверяющего центра, администратор УЦ совместно с уполномоченным лицом удостоверяющего центра производит формирование нового ключа электронной подписи и сертификата ключа проверки электронной подписи уполномоченного лица удостоверяющего центра.

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

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

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

5.7. Восстановление в случае компрометации или аварии

5.7.1. Действия по предотвращению компрометации и аварии

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

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

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

5.7.3. Компрометация ключа участника информационной системы

К событиям, связанным с компрометацией, относятся следующие события:

- потеря ключевых носителей, в том числе с их последующим обнаружением;
- увольнение по любой причине сотрудников, имеющих доступ к ключевым носителям или к ключевой информации на данных носителях (возможность такого доступа определяется в зависимости от конкретной реализации системы со средствами ЭП и от технологии обработки информации данной системой);
- возникновение подозрений об утечке информации или ее искажении в системе;
- нарушение целостности печати на сейфе с ключевыми носителями или утрата контроля за ключом от такого сейфа;
- утрата пользователем контроля за ограничением доступа к ключевому носителю в процессе эксплуатации им системы;

- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем (например, его разрушение и невозможность опровергнуть подозрение на то, что разрушение носителя произошло не в результате попытки доступа к нему злоумышленника);
- другие виды разглашения ключевой информации, в результате которых ключи электронной подписи могут стать доступными несанкционированным лицам и (или) процессам.

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

В случае необходимости отзыва (аннулирования) сертификата выполняется следующая процедура:
- сведения об аннулировании сертификата в связи с компрометацией доводятся до других участников информационных систем путем публикации в списке отозванных сертификатов;
- владелец скомпрометированного ключа электронной подписи письменно уведомляет других участников информационных систем о факте компрометации в случае необходимости;
- владелец скомпрометированного ключа электронной подписи получает новые ключи и сертификат в порядке, указанном в настоящем регламенте.

5.7.4. Восстановление работоспособности после аварии

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

План восстановления работоспособности после аварии предполагает восстановление в течение от 24 до 48 часов таких функций, как:
- выпуск сертификатов;
- отзыв сертификатов.

Публикация списков отозванных сертификатов осуществляется непрерывно.

5.8. Разрешение конфликтных ситуаций

5.8.1. Некорректность входящего электронного документа или электронной подписи

Действия сторон в данной ситуации заключаются в следующем:

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

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

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

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

При этом необходимо:

- проверить сертификаты ключей проверки электронных подписей;

- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения средств ЭП. И переустановить их в случае необходимости.

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

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

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

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

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

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

- данные архива оригиналов принятых/отправленных документов;

- сертификаты ключей проверки электронных подписей, выданные Удостоверяющим Центром;

- дистрибутивы средств ЭП;

- ключевые носители.

Процедура проверки ЭП документа

Для проведения разбора конфликтной ситуации необходимы:

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

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

Для разбора конфликтной ситуации необходимо выполнить следующие действия:

Произвести операцию проверки подписи электронного документа, авторство подписи которого оспаривается на специализированном рабочем месте разбора конфликтных ситуаций.

Распечатать протокол проверки подписи.

Распечатать сертификат ключа проверки электронной подписи из Реестра удостоверяющего центра.

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

Авторство подписи под документом считается установленным, если совпадают ключи проверки электронной подписи представленного сертификата ключа проверки электронной подписи и сертификат ключа проверки

электронной подписи из Реестра удостоверяющего центра, и в протоколе проверки подписи пользователя сформирована запись “Подпись верна”.

5.9. Прекращение работы удостоверяющего центра

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

6. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1. Изготовление и установка ключевой пары

6.1.1. Изготовление ключей

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

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

6.1.2. Передача ключа электронной подписи владельцу

В тех случаях, когда генерацию ключей производит сотрудник УЦ, процедура проводится в присутствии заявителя или его законного представителя. Ключевой носитель с ключами передается владельцу или его законному представителю сразу после выпуска и установки в него сертификата ключа проверки электронной подписи.

6.1.3. Передача ключа проверки электронной подписи в удостоверяющий центр

В тех случаях, когда заявитель осуществляет самостоятельную генерацию ключей, он передает в удостоверяющий центр ключ проверки электронной подписи в составе сообщения формата PKCS#10 в электронном виде с использованием электронных носителей. Для процедуры продления сертификата возможна передача ключа проверки электронной подписи с использованием сообщений электронной почты.

6.1.4. Передача ключей проверки электронных подписей участникам информационных систем

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

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

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

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

6.1.5. Размеры ключей

Размеры ключей электронной подписи:

- ключ электронной подписи – 256 бит;
- ключ проверки электронной подписи – 512 бит

Размеры ключей, используемых при шифровании:
- ключ электронной подписи – 256 бит;
- ключ проверки электронной подписи – 512 бит;
- симметричный ключ – 256 бит;

6.1.6. Параметры генерации и проверки качества ключа электронной подписи
Определяются сертифицированным средством ЭП автоматически.

6.1.7. Цели использования ключа (порядок заполнения поля key usage сертификата x.509v3)
Заполняются в соответствии с политикой сертификата и в сертификатах пользователей могут принимать одно или несколько из перечисленных значений:
- цифровая подпись;
- неотрекаемость;
- шифрование ключей;
- шифрование данных.

6.2. Защита ключа электронной подписи, требования к ключевым носителям и криптографическим модулям
Все действия с ключевыми носителями должны осуществляться строго в соответствии с инструкциями по их эксплуатации и требованиями безопасности.

6.2.1. Требования к ключевым носителям
Допускается использование следующих типов носителей:
- ГМД 3,5’’;
- usb-flash;
- eToken;
- смарт-карты РИК, Оскар, Магистра;
- идентификаторы Touch-Memory DS1995 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь";
- rutoken.

6.2.2. Ключ электронной подписи, контролируемый несколькими держателями (n из m)
В соответствии с эксплуатационной документацией средства ЭП.

6.2.3. Депонирование ключа электронной подписи
Удостоверяющий центр не депонируют ключи электронных подписей.

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

Для некоторых систем ключ электронной подписи может быть неэкспортируемым. Резервное копирование таких ключей не осуществляется.

6.2.5. Архивирование ключа электронной подписи

Ключи электронных подписей с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией средства ЭП. Архивное хранение ключей электронных подписей не допускается.

6.2.6. Запись ключа электронной подписи в криптографический модуль (ключевой носитель)

Производится автоматически средствами ЭП в соответствии с эксплуатационной документацией.

6.2.7. Хранение ключа электронной подписи в криптографическом модуле (ключевом носителе)

Ключи электронных подписей хранятся только в зашифрованном виде.

6.2.8. Способы активации ключа электронной подписи

Все владельцы сертификатов ключей проверки электронных подписей обязаны хранить и защищать свои ключи электронных подписей в соответствии с требованиями эксплуатационной документации средства ЭП и действующим законодательством.

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

6.2.9. Способы деактивации ключа электронной подписи

Ключ деактивируется средством ЭП автоматически после выполнения связанных с его использованием операций или после физического отключения ключевого носителя от персонального компьютера.

6.2.10. Способы уничтожения ключа электронной подписи

Уничтожение ключа электронной подписи производится в соответствии с эксплуатационной документацией средства ЭП.

6.2.11. Оценка криптографического модуля (ключевого носителя)

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

6.3. Другие особенности использования ключей электронной подписи

6.3.1. Архивирование ключей проверки электронных подписей

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

6.3.2. Сроки действия сертификатов и ключей

Срок действия ключа электронной подписи уполномоченного лица удостоверяющего центра составляет 3 года. В течение 1 года 3 месяцев с момента начала срока действия ключа электронной подписи уполномоченного лица удостоверяющего центра, ключ используется для изготовления сертификатов ключей проверки электронных подписей и формирования списков отозванных сертификатов. По истечении 1 года 3 месяцев и до окончания срока действия ключа электронной подписи уполномоченного лица удостоверяющего центра, данный ключ используется исключительно для формирования списков отозванных сертификатов. Срок действия сертификата ключа проверки электронной подписи уполномоченного лица удостоверяющего центра составляет 25 лет.

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

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

6.4. Данные активации ключей электронных подписей

6.4.1. Генерация и установка данных активации ключа электронной подписи

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

К активационным данным (PIN) предъявляются следующие требования:
- смена должна быть произведена владельцем ключевого носителя немедленно после первого подключения к персональному компьютеру;
- не должен быть короче 6 символов;
- должен соответствовать политике паролей организации пользователя;
- рекомендуется производить смену PIN-кода не реже одного раза в три месяца.

6.4.2. Защита данных активации ключа электронной подписи

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

6.4.3. Особенности данных активации ключа электронной подписи

PIN-код аппаратных ключевых носителей (eToken, Rutoken и т.п.) может содержать только цифры и буквы латинского алфавита в различном регистре.

6.5. Меры обеспечения информационной безопасности

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

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

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

7. ПРОФИЛИ СЕРТИФИКАТОВ И CRL

7.1. Профиль сертификата

Сертификаты ключей проверки электронных подписей соответствуют требованиям приказа ФСБ РФ от 27 декабря 2011 г. №795.

Сертификаты ключей проверки электронных подписей содержат следующие базовые поля X.509:

version:	Версия сертификата формата X.509 - версия 3
serialNumber:	Серийный (регистрационный) номер сертификата в Реестре сертификатов ключей проверки электронных подписей УЦ

signature:	Объектный идентификатор алгоритма, с использованием которого сформирована электронная подпись уполномоченного лица УЦ в сертификате
issuer:	Идентифицирующие данные уполномоченного лица УЦ
validity:	Даты начала и окончания срока действия сертификата
subject:	Идентифицирующие данные владельца сертификата ключа подписи
subjectPublicKeyInformation:	Идентификатор алгоритма средства электронной подписи, с которыми используется данный открытый ключ, значение открытого ключа
issuerUniqueIdentifier	Уникальный идентификатор издателя (необязательное)
subjectUniqueIdentifier	Уникальный идентификатор владельца (необязательное)
extensions	Дополнительная информация, касающаяся использования сертификата (расширения сертификата)

7.1.1. Версия сертификата

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

7.1.2. Расширения сертификата

Сертификаты ключей проверки электронных подписей содержат следующие дополнения:

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

7.1.3. Объектные идентификаторы алгоритмов

Удостоверяющий центр использует следующие идентификаторы алгоритмов средства электронной подписи:

ГОСТ Р 34.10-2001	1.2.643.2.2.19
ГОСТ Р 34.11-94	1.2.643.2.2.9

ГОСТ 28147-89	1.2.643.2.2.21
Диффи-Хеллмана	1.2.643.2.2.98

7.1.4. Форматы имен (идентификационных данных)

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

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

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

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

Common Name	Фамилия, имя, отчество
SNILS	Страховой номер индивидуального лицевого счета физического лица
Email	Адрес электронной почты
Country	RU

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

Common Name	Наименование юридического лица
surname	Фамилия физического лица, действующего от имени юридического лица
givenName	Имя и отчество физического лица, действующего от имени юридического лица
locality	Наименование населенного пункта места нахождения юридического лица
street	Адрес места нахождения юридического лица
Organization	Наименование юридического лица
Organization Unit	Наименование подразделения юридического лица

Email	Адрес электронной почты
Country	RU
State	Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата
OGRN	Основной государственный регистрационный номер юридического лица
INN	Индивидуальный номер налогоплательщика юридического лица

7.1.5. Ограничения, накладываемые на имена (идентификационные данные)

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

7.1.6. Объектный идентификатор политики сертификата

Нет условий.

7.1.7. Использование расширения Policy Constraints

Нет условий.

7.1.8. Использование расширения Policy Qualifier

Нет условий.

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

Решение о доверии к сертификату ключа подписи принимается пользователем самостоятельно.

7.2. Профиль CRL

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

7.3. Дополнения CRL

Удостоверяющий центр ПК использует следующие дополнения:

AuthorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
ReasonCode	Код причины отзыва сертификата открытого ключа