УТВЕРЖДЕН
ФРКЕ.00114-01 90 02-ЛУ

Программный комплекс
ViPNet Удостоверяющий центр 4

Типовой регламент функционирования

ФРКЕ.00114-01 90 02

Листов 50

2014

Подп. и дата	
Инв. № дубл.	
Взам. инв.№	
Подп. и дата	
Инв.№ подл.	

АННОТАЦИЯ

Настоящий документ содержит типовой Регламент удостоверяющего центра организации, эксплуатирующей программный комплекс «ViPNet Удостоверяющий центр 4» (далее – ViPNet УЦ).

Деятельность УЦ должна обеспечиваться в соответствии с положениями Федерального закона № 63-ФЗ «Об электронной подписи».

Регламент удостоверяющего центра эксплуатирующей организации должен создаваться с учетом положений настоящего документа, действующего законодательства Российской Федерации, рекомендаций RFC 3647 (Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework).

Информация о разработчике ПК «ViPNet УЦ 4»:

ОАО «ИнфоТеКС»

127287, Москва, Старый Петровско-Разумовский проезд, д.1/23, стр.1

Телефон: (495) 737-61-92

Факс (495) 737-72-78

http://www.infotecs.ru

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ViPNet	Торговая марка программных продуктов компании ОАО «ИнфоТеКС»
CRL	Certificate Revocation List, список аннулированных сертификатов
НСД	Несанкционированный доступ
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

1 ВВЕДЕНИЕ

1.1 Обзорная информация

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего центра (УЦ) _____ (полное наименование юридического лица), включая обязанности пользователей УЦ (см. раздел [4.2] настоящего Регламента) и членов группы администраторов ViPNet УЦ 4, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ.

1.2 Идентификация Регламента

Наименование документа: «Программный комплекс ViPNet «Удостоверяющий центр 4». Типовой регламент функционирования».

Индекс:

Дата: ___.___.20___

Объектный идентификатор: _____.

1.3 Публикация Регламента

Настоящий Регламент распространяется:

- В электронной форме:
  a. из репозитория УЦ по адресу _____ (URL с указанием протокола);
  b. через E-mail от отправителя _____ (адрес электронной почты отправителя)
- В бумажной форме:
  a. через _____ (почтовый адрес доверенного лица УЦ).

Копии Регламента, предназначенные для распространения в электронной форме из репозитория УЦ, распространяются в виде двух файлов, один из которых содержит электронный образ Регламента, а другой − электронную подпись УЦ к файлу электронного образа Регламента.

1.4 Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязанности для всех вовлеченных сторон, а также средством официального уведомления и

информирования всех сторон о 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 1.3 данного Регламента.

1.6 Контактная информация

_____ (полное наименование юридического лица).

_____ (почтовый адрес).

_____ (адрес электронной почты).

_____ (факс).

Контактный телефон Административной службы УЦ _____

E-mail Административной службы УЦ _____

Контактный телефон Службы регистрации УЦ _____

E-mail Службы регистрации УЦ _____

Контактный телефон Службы безопасности УЦ _____

E-mail Службы безопасности УЦ _____

Контактный телефон Технической службы УЦ _____

E-mail Технической службы УЦ _____

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Функции удостоверяющего центра

В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» удостоверяющий центр выполняет следующие функции:

- создает сертификаты ключей проверки электронных подписей (далее − сертификат) и выдает такие сертификаты лицам, обратившимся за их получением (далее − заявитель);
- устанавливает сроки действия сертификатов;
- аннулирует выданные этим удостоверяющим центром сертификаты;
- выдает по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП заявителем;
- ведет реестр выданных и аннулированных этим УЦ сертификатов ключей проверки ЭП (далее − реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим УЦ сертификатах ключей проверки ЭП, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки ЭП и об основаниях таких прекращения или аннулирования;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;
- создает по обращениям заявителей ключи ЭП и ключи проверки ЭП;
- проверяет уникальность ключей проверки ЭП в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку ЭП.

2.2 Услуги, предоставляемые Удостоверяющим центром

В процессе своей деятельности УЦ предоставляет пользователям УЦ следующие виды услуг:

- внесение в реестр Удостоверяющего центра регистрационной информации о владельцах сертификатов;
- изготовление сертификатов ключей проверки ЭП в электронной форме;
- изготовление сертификатов ключей проверки ЭП на бумажном носителе;

- формирование ключей ЭП и ключей проверки ЭП по обращениям заявителей с записью их на ключевой носитель;
- ведение реестра сертификатов, выпущенных в данном УЦ;
- предоставление в электронной форме сертификатов, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
- аннулирование сертификатов по обращениям владельцев сертификатов;
- ведение списков аннулированных сертификатов (CRL) и предоставление доступа к ним пользователям УЦ;
- подтверждение подлинности ЭП в документах, представленных в электронной форме, по обращениям пользователей УЦ;
- подтверждение подлинности ЭП доверенного лица УЦ в изготовленных им сертификатах ключей проверки ЭП по обращениям пользователей УЦ;
- распространение средств ЭП по обращениям пользователей УЦ.

2.3 Разграничение полномочий в Удостоверяющем центре

В УЦ должны быть сформированы следующие роли:

- роль «Системный администратор УЦ». Данную роль исполняют следующие группы администраторов:
  - группа Администраторов безопасности;
  - группа Системных администраторов УЦ;
- роль «Администратор сертификации УЦ». Данную роль исполняет Администратор УЦ;
- роль «Администратор Центра регистрации». Данную роль исполняет группа Администраторов Центра регистрации.

Для обеспечения безопасной эксплуатации вспомогательного ПО должна быть сформирована роль «Администратор вспомогательного ПО», которую исполняет группа Администраторов Сервисов публикации. При необходимости (если вспомогательное ПО установлено на компьютерах, на которых не развернуты средства УЦ) допускается ввод в организации дополнительных групп Администраторов вспомогательного ПО.

2.3.1 Группа Администраторов средств УЦ

2.3.1.1 Группа Администраторов безопасности

Администратор безопасности выполняет следующие функции:

- несет ответственность за соблюдением правил безопасной эксплуатации комплекса в целом;
- обеспечивает синхронизацию времени на серверах времени и контроль синхронизации времени на компьютерах пользователей;
- осуществляет контроль над соблюдением правил эксплуатации и соблюдением мер защиты от НСД;
- осуществляет проверку целостности ПО компонентов УЦ;
- осуществляет аудит событий по журналам программных компонентов УЦ, журналам операционной системы и аппаратных средств защиты от НСД;
- контролирует целостность журналов и архивов журналов.

Для обеспечения своих функций Администратор безопасности должен иметь выделенную учетную запись для входа в ОС с правами администратора.

2.3.1.2 Группа системных администраторов УЦ

Системный администратор УЦ выполняет следующие функции:

- инсталляция, конфигурация и поддержка функционирования средств УЦ;
- создание и поддержка профилей членов группы Администраторов средств УЦ;
- конфигурация профиля и параметров журнала аудита;
- осуществляет настройки ОС и прикладного ПО.

Для обеспечения своих функций системный администратор должен иметь выделенную учетную запись для входа в ОС с правами администратора.

2.3.1.3 Администратор УЦ

Администратор УЦ выполняет роль Администратора сертификации средств УЦ с основными обязанностями: создание и аннулирование сертификатов. В рамках одного удостоверяющего центра может быть только один администратор УЦ, который является доверенным лицом УЦ.

Администратор УЦ выполняет следующие функции:

- обеспечивает генерацию ключей ЭП, ключей проверки ЭП, ключей шифрования;
- осуществляет издание сертификатов по запросам на издание или обновление;
- осуществляет проведение работ по отзыву, приостановлению и возобновлению сертификатов пользователей;
- по обращениям заявителей осуществляет проверку ЭП в электронных документах и проверку ЭП в сертификате ключа проверки ЭП;

- при необходимости осуществляет настройку системы информирования (ViPNet CA Informing);
- осуществляет своевременное создание архивов баз данных и восстановление их при сбоях;
- осуществляет настройку журналов УКЦ;
- осуществляет ведение документации УЦ согласно должностным инструкциям сотрудников УЦ;
- осуществление рассылки уведомлений о событиях, связанных с сертификатами, выпущенными данным УЦ, формирование отчетов, позволяющих предоставлять информацию о сертификатах.

Для обеспечения своих функций Администратор УЦ должен:

- быть зарегистрирован на СУ, на котором установлено ПО ViPNet Administrator Удостоверяющий и ключевой центр;
- обладать паролем входа в ОС с правами, достаточными для выполнения своих обязанностей;
- обладать паролем для входа в программу ViPNet УКЦ и иметь доступ к ее рабочим каталогам.

2.3.1.4 Группа Администраторов Центра регистрации

Администратор ViPNet Registration Point выполняет следующие функции:

- осуществляет регистрацию пользователей;
- создает запросы на издание, обновление и отзыв сертификатов пользователей;
- осуществляет, при необходимости, проверку сертификатов пользователей;
- осуществляет настройку интерфейса для автоматизированной обработки и передачи в УЦ запросов на издание сертификатов.

Для обеспечения своих функций Администратор ViPNet Registration Point должен:

- быть зарегистрирован на СУ, на котором установлено ПО ViPNet Registration Point;
- иметь действительный ключ ЭП и сертификат для подписи запросов к УЦ;
- обладать паролем входа в ОС с правами, достаточными для выполнения своих обязанностей;
- обладать паролем входа в программу ViPNet Registration Point и иметь доступ к ее рабочим каталогам.

2.3.2 Группа Администраторов вспомогательного ПО

2.3.2.1 Группа Администраторов Сервиса публикации

Администратор ViPNet Publication Service выполняет следующие функции:

- обеспечивает публикацию изданных сертификатов, а также списков аннулированных сертификатов в выбранных хранилищах данных;
- определяет точки опроса для импорта списков аннулированных сертификатов доверенных УЦ;
- осуществляет контроль опубликованных данных;
- обеспечивает доступ к сертификатам и спискам аннулированных сертификатов.

Для обеспечения своих функций Администратор ViPNet Publication Service должен

- быть зарегистрирован на СУ, на котором установлено ПО ViPNet Publication Service;
- обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей.

2.4 Разрешение споров

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и пользователь УЦ (владелец сертификата, выпущенного данным 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.

2.5 Платность услуг

Услуга Удостоверяющего центра по предоставлению списков аннулированных сертификатов и сертификатов в электронной форме, находящихся в реестре изготовленных сертификатов, предоставляется на безвозмездной основе.

Состав и стоимость предоставляемых дополнительных услуг определяется УЦ.

2.6 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.

2.7 Прекращение деятельности

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

2.8 Порядок утверждения и внесения изменений в Регламент

Регламент составляется в электронном виде. Печатная копия заверяется собственноручной подписью доверенного лица (администратора) УЦ и печатью УЦ.

Изменения в Регламент вносятся путем составления дополнительного соглашения к Регламенту.

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

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

3 ПРАВА

3.1 Права Удостоверяющего центра

Удостоверяющий центр имеет право:

- предоставлять в электронной форме сертификаты, находящихся в реестре Удостоверяющего центра, всем лицам, обратившимся в Удостоверяющий центр;
- отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
- отказать в изготовлении ключей незарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;
- отказать в изготовлении сертификата зарегистрированным пользователям УЦ, подавшим заявление на его изготовление, с указанием причин отказа;
- отказать в аннулировании сертификата владельцу сертификата, подавшему заявление на аннулирование сертификата, в случае если истек установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;
- аннулировать сертификат пользователя УЦ в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата и указанием обоснованных причин.

3.2 Права пользователей УЦ

Пользователи имеют следующие права:

- получить и применять сертификат доверенного лица УЦ для проверки ЭП доверенного лица УЦ в сертификатах ключей проверки ЭП, изданных УЦ;
- получить и применять список аннулированных сертификатов для установления статуса сертификатов ключей проверки ЭП, изданных УЦ;
- получить и применять копию сертификата в электронной форме, находящегося в реестре сертификатов УЦ, для проверки ЭП;
- получить на бумажном носителе сертификат ключа проверки ЭП, заверенный подписью доверенного лица УЦ;
- обратиться в УЦ с заявлением на выполнение УЦ действий, предусмотренных настоящим регламентом.

4 ОБЯЗАННОСТИ

4.1 Обязанности Удостоверяющего центра

4.1.1 Аудит

УЦ обязан осуществлять проверку на предмет соответствия деятельности УЦ требованиям настоящего Регламента и предоставлять необходимые материалы для проверки.

Проверка УЦ должна проводиться не реже одного раза в год.

Для проведения проверок привлекается организационно или юридически независимое от проверяемого УЦ лицо, имеющего необходимые средства, навыки и умения.

4.1.2 Изготовление ключа ЭП доверенного лица УЦ

УЦ обязан изготовлять ключ ЭП доверенного лица. Для изготовления ключа ЭП доверенного лица УЦ и формирования ЭП используется только средство ЭП ViPNet CSP 4, сертифицированное по классу КС2 и КС3 требований ФСБ России, и указанные в документации на него ключевые носители.

Ключ ЭП доверенного лица УЦ должен использоваться только для подписи издаваемых им сертификатов и списков аннулированных сертификатов.

УЦ обязан принимать меры по защите ключа ЭП доверенного лица УЦ.

4.1.3 Синхронизация времени

УЦ обязан синхронизировать по времени все программные и технические средства обеспечения деятельности удостоверяющего центра.

4.1.4 Регистрация пользователей УЦ

УЦ обеспечивает регистрацию пользователей УЦ по заявлениям на регистрацию (порядок регистрации изложен в настоящем Регламенте).

УЦ не имеет права разглашать (публиковать) регистрационную информацию пользователей УЦ, за исключением информации, заносимой в изготавливаемые сертификаты.

4.1.5 Изготовление ключей ЭП и ключей проверки ЭП пользователей УЦ

УЦ обязан изготовить ключ ЭП и ключ проверки ЭП зарегистрированному пользователю УЦ по его заявлению.

УЦ обязан обеспечить сохранение в тайне изготовленного ключа ЭП пользователя.

В соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей, УЦ обязан выполнять процедуру генерации ключей на отделяемых ключевых носителях только с использованием сертифицированных программных и/или аппаратных средств.

4.1.6 Изготовление сертификатов

УЦ обеспечивает изготовление сертификата зарегистрированному пользователю УЦ по его заявлению (формат и порядок идентификации владельца сертификата определен в настоящем Регламенте).

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

4.1.7 Аннулирование сертификатов

УЦ обязан аннулировать сертификат по заявлению его владельца.

УЦ обязан в течение 24 часов занести сведения об аннулированном сертификате в список аннулированных сертификатов (CRL) с указанием даты и времени занесения в CRL.

4.1.8 Уведомления

4.1.8.1 Уведомление о факте изготовления сертификата

УЦ обязан официально уведомить о факте изготовления сертификата его владельца.

Срок уведомления – не позднее 24 часов с момента изготовления.

4.1.8.2 Уведомление о факте аннулирования сертификата

УЦ обязан официально уведомить о факте аннулирования сертификата его владельца.

Срок уведомления – не позднее 24 часов с момента занесения сведений об аннулированном сертификате в список аннулированных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате.

Временем аннулирования сертификата признается время занесения сведений об аннулированном сертификате в список аннулированных сертификатов и включенное в его структуру.

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

УЦ обязан включать полный адрес (URL) списка аннулированных сертификатов в издаваемые сертификаты пользователей УЦ.

4.1.9 Ведение реестра сертификатов

УЦ обязан вести реестр всех изготовленных сертификатов в течение установленного срока хранения.

Реестр сертификатов ведется в электронном виде.

Удостоверяющий центр обязан публиковать выписки из реестра, позволяющие определить действительность сертификатов пользователей УЦ.

Выписка из реестра УЦ предоставляется по требованию пользователя в виде списка сертификатов и, при необходимости, списка аннулированных сертификатов в электронной форме в формате X.509.

4.1.10 Прочие обязанности

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

4.2 Обязанности пользователей УЦ

4.2.1 Обязанности лиц, проходящих процедуру регистрации в УЦ

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

4.2.2 Обязанности пользователей УЦ

Владелец ключа ЭП обязан:

- хранить в тайне ключи ЭП, принимать все возможные меры для предотвращения потери, раскрытия, модифицирования или несанкционированного использования;
- не использовать ключ ЭП, если есть основания полагать, что конфиденциальность данного ключа нарушена;
- использовать ключ ЭП только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;

- в случае компрометации ключа ЭП немедленно сообщить об этом в УЦ доверенному лицу (администратору УЦ);
- не использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, который аннулирован, действие которого прекращено или приостановлено;
- использовать для создания и проверки ЭП, создания ключей ЭП и ключей проверки ЭП средства ЭП, сертифицированные по требованиям ФСБ России.

5 ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

5.1 Типы конфиденциальной информации УЦ

Ключ ЭП является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки ЭП. УЦ не осуществляет хранение ключей ЭП пользователей УЦ.

Персональная и корпоративная информация о пользователях УЦ, не являющаяся частью сертификата ключа проверки ЭП, считается конфиденциальной.

5.2 Типы информации УЦ, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, является открытой информацией.

Открытая информация может публиковаться по решению УЦ.

Место, способ и время публикации также определяется решением УЦ.

Информация, включаемая в сертификаты пользователей УЦ и списки аннулированных сертификатов, издаваемых УЦ, не считается конфиденциальной.

Также не считается конфиденциальной информация, содержащаяся в настоящем Регламенте.

5.3 Исключительные полномочия УЦ

УЦ 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 или при наличии судебного постановления.

6 ПРОЦЕДУРЫ И МЕХАНИЗМЫ

6.1 Сценарии взаимодействия пользователей с удостоверяющим центром

Возможны следующие сценарии получения ключей ЭП и сертификата в Удостоверяющем центре:

1. Пользователь самостоятельно формирует при помощи сертифицированного СКЗИ пару ключей и запрос на издание сертификата в формате PKCS#10 и приносит данный запрос в ЦР. Администратор ЦР проверяет запрос, регистрирует пользователя, подписывает запрос своим ключом и отправляет в ViPNet УКЦ, где администратор УЦ просматривает и обрабатывает запрос. Сертификат издается и отправляется обратно в ЦР. Администратор ЦР передает изданный сертификат заявителю в электронном виде. Также заявителю администратор ЦР выдает заверенный личной подписью сертификат на бумажном носителе. Заявитель проверяет правильность данных и заверяет сертификат своей личной подписью.
2. Пользователь обращается с личным заявлением в ЦР. Администратор ЦР регистрирует пользователя, самостоятельно формирует запрос на издание сертификата и пару ключей. Ключ ЭП создает непосредственно на ключевом носителе. Далее администратор ЦР подписывает запрос и отправляет его в ViPNet УКЦ. Администратор УЦ просматривает запрос и издает сертификат. Изданный сертификат отправляется обратно в ЦР. Администратор ЦР полученный сертификат сохраняет в контейнер на ключевой носитель, с уже имеющимся там ключом ЭП, и передает данный носитель заявителю. Также заявителю администратор ЦР выдает заверенный личной подписью сертификат на бумажном носителе. Заявитель проверяет правильность данных и заверяет сертификат своей личной подписью.

6.2 Процедура регистрации пользователей УЦ

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

6.2.1 Заявление на регистрацию

Лицо (заявитель), желающее пройти процедуру регистрации в УЦ, должно подать заявление на регистрацию в простой письменной форме, заверенное собственноручной подписью, в УЦ.

Заявление должно содержать следующие обязательные реквизиты:

Для физического лица:

- идентификационные данные, включающие:
  - фамилию, имя и отчество;
  - СНИЛС (страховой номер индивидуального лицевого счета владельца квалифицированного сертификата);
  - адрес электронной почты;
- контактные телефоны.

Для физического лица, представляющего юридическое лицо:

- идентификационные данные, включающие:
  - наименование организации;
  - ИНН (идентификационный номер налогоплательщика) организации;
  - ОГРН (основной государственный регистрационный номер) организации;
  - адрес места нахождения организации;
  - фамилию, имя и отчество лица, представляющего организацию;
  - СНИЛС лица, представляющего организацию;
  - должность полномочного представителя;
  - наименование подразделения полномочного представителя
  - адрес электронной почты полномочного представителя;
  - субъект Российской Федерации, в котором зарегистрирована организация;
- данные доверенности (или других документов, подтверждающих правомочность действий от имени юридического лица).

Дополнительно (определяется заявителем) заявление может содержать следующую информацию, включаемую в идентификационные данные:

- псевдоним;
- почтовый и/или юридический адрес.

К заявлению физического лица, представляющего юридическое лицо, прилагаются оригинал доверенности или копии документов, подтверждающих правомочность действий от имени юридического лица.

Для физического лица, представляющего индивидуального предпринимателя:

- идентификационные данные, включающие:
  - фамилию, имя и отчество;
  - адрес электронной почты;
  - наименование ИП;
  - субъект Российской Федерации, в котором зарегистрирован ИП;

- ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя);
- ИНН (идентификационный номер налогоплательщика) ИП;

– данные доверенности (или других документов, подтверждающих правомочность действий от имени индивидуального предпринимателя).

Дополнительно (определяется заявителем) заявление может содержать следующую информацию, включаемую в идентификационные данные:

- псевдоним;
- почтовый и/или юридический адрес.

К заявлению физического лица, представляющего индивидуального предпринимателя, прилагаются оригинал доверенности или копии документов, подтверждающих правомочность действий от имени индивидуального предпринимателя.

6.2.2 Идентификация пользователя УЦ

Идентификация пользователя выполняется в процессе его регистрации в Центре регистрации в качестве пользователя УЦ в реестре УЦ.

Результатом идентификации является присвоение пользователю УЦ идентификатора и занесение идентификатора в реестр пользователей УЦ.

Идентификатором зарегистрированного пользователя являются идентификационные данные из заявления на регистрацию (см. раздел [6.2.1] настоящего Регламента).

6.2.3 Регистрация пользователя УЦ, обработка запроса на издание сертификата

Регистрация пользователя УЦ осуществляется администратором Центра регистрации на основании заявления на регистрацию при личном прибытии лица, проходящего процедуру регистрации, в офис УЦ.

Администратор ЦР проверяет состав, полноту и корректность оформления Заявления и соответствие указанных в нем данных предоставленным документам, а также осуществляет аутентификацию заявителя.

При положительном результате проверки и аутентификации администратор ЦР выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по паспорту или иному документу, удостоверяющему личность.

Заявление на регистрацию рассматривается в УЦ в течение 2 рабочих дней с момента поступления.

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

При принятии положительного решения возможны два варианта изготовления ключей ЭП и издания сертификата:

1. Пользователь самостоятельно формирует пару ключей и запрос на издание сертификата в формате PKCS#10 (например, с помощью СКЗИ ViPNet CSP) и передает данный запрос в ЦР. Администратор ЦР проверяет запрос, регистрирует пользователя, подписывает запрос своим ключом и отправляет в ViPNet УКЦ, где запрос обрабатывается, издается сертификат и отправляется обратно в ЦР. Администратор ЦР экспортирует сертификат в файл в формате стандарта Cryptographic Massage Syntax, включив все сертификаты в путь сертификата, и передает изданный сертификат заявителю.
2. Администратор ЦР регистрирует пользователя, самостоятельно формирует запрос на издание сертификата и пару ключей. Ключ ЭП создает непосредственно на ключевом носителе. Далее администратор подписывает запрос и отправляет его в ViPNet УКЦ, где запрос обрабатывается, издается сертификат и отправляется обратно в ЦР. Администратор ЦР полученный сертификат сохраняет в контейнер на ключевой носитель, с уже имеющимся там ключом ЭП, и передает данный носитель заявителю.

Также заявителю администратор ЦР выдает заверенный личной подписью сертификат на бумажном носителе. Заявитель проверяет правильность данных и заверяет сертификат своей личной подписью.

По необходимости, регистрируемый пользователь УЦ должен приобрести (получить) средство ЭП и шифрования, распространяемое УЦ.

6.3 Идентификация зарегистрированного пользователя

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

6.4 Аутентификация зарегистрированного пользователя

6.4.1 Очная аутентификация зарегистрированного пользователя

Очная аутентификация зарегистрированного пользователя УЦ выполняется по паспорту или другому документу, удостоверяющего личность, предъявляемого лично.

6.4.2 Аутентификация зарегистрированного пользователя по сертификату

Аутентификация зарегистрированного пользователя УЦ по сертификату выполняется путем выполнения процедуры подтверждения ЭП с использованием сертификата (см. п. 6.10 настоящего Регламента).

6.5 Изготовление ключей подписи

Изготовление ключей ЭП и ключей проверки ЭП (ключей подписи) осуществляется в УЦ по обращению пользователей УЦ. Обращение пользователей оформляется в форме заявления на изготовление ключей подписи. Прием заявлений, изготовление и выдача ключей подписи осуществляется администратором ЦР при личном присутствии лица, обратившегося с заявлением.

6.5.1 Заявление на изготовление ключей подписи

Заявление на изготовление ключей подписи подается заявителем в простой письменной форме на бумажном носителе и заверяется собственноручной подписью заявителя.

Заявление на изготовление ключей подписи оформляется заявителем либо по образцу, предоставляемому УЦ либо по бланку, подготавливаемому сотрудником УЦ.

Заявление на изготовление ключей подписи рассматривается УЦ в течение 3 рабочих дней с момента поступления.

6.5.2 Изготовление и выдача ключей подписи владельцу

Изготовление ключей подписи выполняется администратором ЦР на основании принятого заявления.

Изготовленные ключи подписи записываются на ключевой носитель, предоставляемый заявителем или распространяемый УЦ. Ключевой носитель должен соответствовать требованиям, указанным в документации на сертифицированное по требования ФСБ России средство ЭП.

Ключевой носитель, содержащий изготовленные ключи подписи, передается владельцу (заявителю). Факт выдачи ключей заносится в Журнал учета изготовления и выдачи ключей подписи под роспись владельца.

6.6 Изготовление сертификата и предоставление его владельцу

Изготовление сертификата осуществляется в УЦ на основании заявления в соответствии с запросом на изготовление сертификата пользователя УЦ.

Заявление на изготовление сертификата в письменной форме подается заявителем в УЦ лично.

Издание сертификата осуществляется после получения и обработки в УЦ сформированного запроса (см. п. 6.5.1).

За проверку данных запроса с последующим выпуском сертификата ответственным является администратор ЦР.

Сертификаты, изданные в ViPNet УЦ, имеют структуру формата X.509 с дополнениями из рекомендаций RFC 4491. Изданные квалифицированные сертификаты соответствуют требованиям, изложенным в приказе ФСБ России №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Срок рассмотрения заявления на изготовление сертификата составляет 3 рабочих дня с момента его поступления в УЦ.

После изготовления сертификата его владельцу направляется официальное уведомление (см. раздел [4.1.8] настоящего Регламента).

Изготовленный сертификат в электронной форме, заверенный ЭП доверенного лица УЦ, предоставляется его владельцу при личном обращении в УЦ. Также предоставляется сертификат на бумажном носителе, заверенный подписью администратора ЦР.

По окончании процедуры изготовления сертификата пользователь УЦ получает:

- сертификат в электронной форме;
- сертификат на бумажном носителе;
- сертификат доверенного лица УЦ в электронной форме;
- ключи ЭП, записанные на ключевой носитель (в случае если ключи формировались администратором ЦР, а не самим заявителем).

6.6.1 Заявление и запрос на изготовление сертификата

Заявление на изготовление сертификата в письменной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

- фамилию, имя, отчество заявителя;
- дата и подпись заявителя;
- текст запроса на сертификат;
- доверенность (при необходимости).

В ViPNet УЦ сертификаты издаются либо при создании дистрибутивов ключей, либо на основе запросов двух форматов: PKCS#10 и SOK (формат используется только в продуктах ViPNet).

В формате PKCS#10 поступают запросы на сертификаты, переданные в ViPNet УКЦ непосредственно пользователями. Запросы такого формата считаются самоподписанными, поскольку подпись таких запросов выполнена на ключах подписи, соответствующих ключам проверки подписи внутри запросов. Подпись подтверждает, что пользователь, передавший запрос, является обладателем ключа подписи.

Запросы на сертификаты в формате SOK поступают в ViPNet УКЦ из центров регистрации. Запрос в формате SOK представляют хранилище сертификатов с объектом, имеющим структуру сертификата X.509. Запросы такого формата заверены сертификатом Администратора Центра регистрации. При поступлении такого запроса на обработку проверяется владелец сертификата, которым он был подписан. Если владелец подтверждается и сертификат действителен, то запрос принимается на обработку.

В других форматах запросы на сертификат в УЦ не принимаются.

6.6.2 Идентификация владельца сертификата

Владелец сертификата идентифицируется по значениям атрибутов поля Subject сертификата (см. раздел [8.1] настоящего Регламента).

6.7 Аннулирование сертификата

Заявление на аннулирование сертификата в письменной форме подается заявителем в УЦ лично.

Срок рассмотрения заявления на аннулирование сертификата составляет один рабочий день с момента его поступления в УЦ.

УЦ может по собственной инициативе аннулировать сертификат пользователя УЦ в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата указанием обоснованных причин отзыва.

Администратор ЦР формирует запрос на отзыв сертификата, подписывает его и отправляет в ViPNet УКЦ, где запрос обрабатывается администратором УЦ и сертификат попадет в список аннулированных сертификатов администратора УЦ (издателя сертификата) и будет иметь статус **Отозван**. Данный CRL поступает администратору ЦР (в программу ViPNet Registration Point) вместе с ответом на запрос об отзыве сертификата. С момента получения остальными пользователями обновленного CRL аннулированный сертификат станет недействительным.

После аннулирования сертификата его владельцу направляется официальное уведомление (см. раздел [4.1.8] настоящего Регламента).

6.7.1 Заявление на аннулирование сертификата

Заявление на аннулирование сертификата в письменной форме 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.

6.7.2 Протоколы аннулирования сертификатов

В ViPNet УЦ информация об аннулированных сертификатах предоставляется пользователям путем предоставления списка аннулированных сертификатов (CRL).

6.8 Проверка сертификата по заявлению пользователя

Проверка сертификата осуществляется УЦ по обращению пользователей, на основании заявления в простой письменной форме, или в электронном виде. Заявление на подтверждение электронной подписи в сертификате ключа проверки ЭП подается заявителем в Удостоверяющий центр лично.

Подтверждение подлинности электронной подписи в сертификате ключа проверки ЭП производится администратором Центра регистрации средствами ОС при проведении технической экспертизы. Обязательным приложением к заявлению на подтверждение ЭП в сертификате ключа проверки ЭП является цифровой носитель, содержащий сертификат ключа проверки ЭП (с расширением .cer) зарегистрированного пользователя Удостоверяющего центра, подвергающийся процедуре проверки.

Срок рассмотрения заявления на подтверждение ЭП в сертификате ключа проверки ЭП зарегистрированного пользователя Удостоверяющего центра составляет 5 рабочих дней с момента поступления заявления в Удостоверяющий центр.

В случае ненадлежащего оформления заявления, отсутствия обязательных файлов или неподтверждения факта издания сертификата пользователя данным Удостоверяющим центром, Удостоверяющий центр имеет право отказать в проведении технической экспертизы. В таком случае заявителю возвращается заявление с соответствующей

резолюцией уполномоченного лица Удостоверяющего центра.

В случае принятия положительного решения по заявлению на подтверждение ЭП в сертификате ключа проверки ЭП заявителю по результатам экспертизы предоставляется ответ в виде протокола проведения технической экспертизы, подписанный собственноручной подписью администратора ЦР.

Порядок проведения технической экспертизы: администратор ЦР открывает сертификат, подвергающийся процедуре проверки. На вкладке «Путь сертификации» в поле «Состояние сертификата» будет отображен статус сертификата. Далее администратор ЦР заполняет Протокол проведения технической экспертизы, в котором отображает результат проверки сертификата.

6.9 Срок хранения сертификата

Хранение сертификата пользователей УЦ в реестре сертификатов УЦ осуществляется в течение установленного срока действия сертификата.

Срок архивного хранения сертификата определен в разделе [7.9] настоящего Регламента.

6.10 Процедура подтверждения ЭП с использованием сертификата

Подтверждение ЭП в электронном документе осуществляется УЦ по обращению граждан (заявителей) в соответствии с «Порядком проверки электронных подписей».

6.11 Механизм доказательства обладания ключом ЭП

Заявления на изготовление сертификатов ключей подписи, поступающие в Удостоверяющий центр от владельцев ключей ЭП и ключей проверки, должны содержать собственноручную подпись заявителя. При первом издании сертификата для данного пользователя ключ ЭП и ключ проверки ЭП формируются непосредственно в Удостоверяющем центре или Центре регистрации. В этом случае факт обладания ключом ЭП подтверждается актом передачи пользователю ключевого носителя.

В случае если ключ ЭП формировался пользователем, в Удостоверяющий центр направляется запрос, подписанный действующим на момент создания запроса ключом ЭП. В трехдневный срок с момента получения изданного сертификата пользователь обязан подтвердить факт обладания ключом ЭП путем отправки подписанного сообщения администратору Удостоверяющего центра. Положительный результат проверки подписи средствами Удостоверяющего центра подтверждает, что заявитель является владельцем ключа

ЭП, которому соответствует ключ проверки ЭП. В случае отсутствия подтверждения администратор имеет право отозвать изданный сертификат.

6.12 Проверка уникальности ключей подписи

При рассмотрении запросов пользователей на издание сертификатов производится проверка на наличие изданных сертификатов, содержащих ключ проверки ЭП, идентичный ключу, содержащемуся в запросе. При обнаружении таких сертификатов ключей проверки ЭП проверяется наличие в базе данных запросов, идентичных входящему. В зависимости от результата проверки выполняются следующие действия:

- если обнаружен запрос, идентичный входящему, он автоматически удаляется из системы без уведомления;
- если запрос уникален, но обнаружен изданный сертификат с идентичным ключом проверки ЭП, запрос отклоняется, и отклоненный запрос отправляется пользователю.

6.13 Проверка соответствия сертификатов и списков аннулированных сертификатов рекомендациям X.509

Сертификаты и списки аннулированных сертификатов издаются УЦ в соответствии со стандартом X.509 [«Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».]. Контроль корректности объектов осуществляется администратором УЦ (или администратором Центра регистрации при его наличии) с использованием встроенных механизмов операционной системы Windows. Для проведения проверки сертификат должен быть экспортирован в файл с расширением *.cer (список аннулированных сертификатов в файл с расширением *.crl). Системная утилита просмотра объекта вызывается при двойном клике мыши на выделенном файле в окне обозревателя ОС Windows.

Критериями корректности являются:

- отсутствие сообщений об ошибках при экспорте объекта и при вызове утилиты просмотра объекта;
- корректное отображение объекта системной утилитой;
- соответствие состава и содержания полей и расширений при просмотре техническими средствами УЦ и средствами ОС.

7 ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1 Идентифицирующие данные доверенного лица УЦ

Доверенное лицо УЦ идентифицируется по следующим данным:

- фамилия, имя, отчество: _____
- организация: _____
- подразделение: _____
- ИНН: _____
- ОГРН: _____
- адрес электронной почты: _____
- субъект Российской Федерации: _____

7.2 Сроки действия ключей доверенного лица УЦ

Сроки действия ключей ЭП доверенного лица (администратора) УЦ составляет 1 год и 3 месяца.

Под сроком действия в данном случае понимается срок использования ключа для подписи издаваемых сертификатов пользователей, но не для подписи CRL. При смене старый ключ подписи не следует удалять, поскольку он будет использоваться для подписи CRL. Подписывать CRL в течение всего времени действия сертификата администратора необходимо для того, чтобы была возможность отзывать пользовательские сертификаты.

Начало действия ключа ЭП доверенного лица (администратора) УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

В соответствии с требованиями Приказа ФСБ России № 796 от 27 декабря 2011 года о том, что срок действия ключа проверки ЭП не должен превышать срок действия соответствующего ключа ЭП более чем на 15 лет, максимально допустимый срок действия сертификата Администратора УЦ составляет 16 лет.

7.3 Требования к средствам ЭП

Средства ЭП – средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.

Согласно части 2 и 3 статьи 12 Федерального закона «Об электронной подписи» средства ЭП должны:

1) При создании ЭП:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;
- однозначно показывать, что ЭП создана.

2) При проверке ЭП:

- показывать содержание электронного документа, подписанного ЭП;
- показывать информацию о внесении изменений в подписанный ЭП электронный документ;
- указывать на лицо, с использование ключа ЭП которого подписаны электронные документы.

Средство ЭП должно обеспечивать выполнение мер защиты ключей ЭП (см. раздел [7.6] настоящего Регламента).

Средства ЭП должны быть сертифицированы в соответствии с «Требованиями к средствам электронной подписи» ФСБ России.

7.4 Сроки действия ключей ЭП и сертификатов ключей проверки ЭП

Сроки действия ключей ЭП составляет 1 год и 3 месяца.

В соответствии с требованиями Приказа ФСБ России № 796 от 27 декабря 2011 года о том, что срок действия ключа проверки ЭП не должен превышать срок действия соответствующего ключа ЭП более чем на 15 лет, максимально допустимый срок действия сертификата пользователя – 15 лет.

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

Срок действия сертификата устанавливается УЦ в момент его изготовления.

7.5 Назначение ключа ЭП, ключа проверки ЭП и сертификата

Ключ ЭП, ключ проверки ЭП и сертификат предназначены для:

- обеспечения аутентификации и авторизации зарегистрированного пользователя УЦ при использовании ПО зарегистрированного пользователя УЦ, предоставляемого УЦ;
- формирования ЭП в заявлении на сертификат в электронном виде;
- использования в областях, указанных в сертификате.

7.6 Меры защиты ключей ЭП

Ключи ЭП пользователей УЦ должны записываться при их генерации на носители ключевой информации. Допустимые носители ключевой информации указаны в документации на СКЗИ.

Ключи ЭП на съемном носителе защищаются паролем (ПИН-кодом), сформированным лицом, выполняющим процедуру генерации ключей, учитывая следующие требования:

- длина пароля (ПИН-кода) не должна быть меньше 8 символов;
- срок действия пароля (ПИН-кода) – не более 6 месяцев;
- пароль (ПИН-код) должен содержать символы цифр и букв латинского алфавита.

Если процедуру генерации ключей подписи пользователя УЦ выполняет администратор УЦ, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключей ЭП.

Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на пользователя ключей ЭП.

Не допускается использовать одно и тоже значение пароля (ПИН-кода) для защиты нескольких ключей ЭП.

Администратор УЦ, являющийся владельцем ключей ЭП, также выполняет указанные в разделе меры защиты ключей ЭП.

7.7 Сертификат ключа проверки ЭП в электронной форме

Сертификат ключа проверки ЭП пользователя УЦ в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту X.509 [«Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».], представленный в кодировке Der или Base64.

7.8 Сертификат ключа проверки ЭП на бумажном носителе

Сертификат ключа проверки ЭП пользователя УЦ на бумажном носителе, представляет собой документ, заверенный личной подписью доверенного лица УЦ, содержащий следующие обязательные реквизиты:

- серийный номер сертификата ключа проверки ЭП;
- срок действия сертификата ключа проверки ЭП;
- сведения о владельце сертификата (идентификационные данные владельца сертификата; ИНН (индивидуальный номер налогоплательщика), СНИЛС

(страховой номер индивидуального лицевого счета) для владельца – физического лица; ИНН и ОГРН (основной государственный регистрационный номер) для владельца – юридического лица; ИНН, СНИЛС и ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) для владельца – индивидуального предпринимателя и др.);

- сведения об издателе сертификата (идентификационные данные издателя сертификата, наименование УЦ, место нахождения УЦ, доверенное лицо УЦ, номер сертификата УЦ и др.);
- сведения о ключе проверки ЭП (используемый алгоритм, класс средства ЭП, область использования ключа, значение ключа и др.);
- ЭП под сертификатом (используемый алгоритм, значение ЭП);
- собственноручная подпись доверенного лица УЦ;
- печать УЦ.

Сертификат ключа проверки ЭП на бумажном носителе печатается на листах белой бумаги формата А4, не содержащих средств защиты от копирования и подделки.

Все поля сертификата отображаются в виде, пригодном для восприятия человеком. Информация о наименованиях, именах, месте нахождения, области применения и другая информация отображается на русском языке с использованием символов кириллического алфавита. Такое отображение информации сертификата позволяет провести процедуру контроля соответствия сертификата в формах электронного документа и документа на бумажном носителе. Контроль соответствия сертификата осуществляется путем сравнения содержимого каждого поля сертификата на бумажном носителе и в электронном виде. При передаче пользователю сертификата ключа проверки ЭП на бумажном носителе администратор УЦ должен проверить идентичность значений полей сертификата в электронной форме и на бумажном носителе.

7.9 Архивное хранение документированной информации

7.9.1 Состав архивируемых документов

Архивированию подлежат следующая документированная информация:

- реестр сертификатов пользователей УЦ;
- сертификаты доверенного лица (администратора) УЦ;
- журналы аудита средств УЦ;
- реестр зарегистрированных пользователей УЦ;

- заявления на изготовление ключей пользователей УЦ;
- заявления на изготовление сертификатов пользователей УЦ;
- заявления на аннулирование сертификатов;
- служебные документы УЦ.

7.9.2 Источник комплектования архивного фонда

Источником комплектования архивного фонда УЦ являются подразделения УЦ, 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, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов устанавливается в соответствии с законодательством Российской Федерации.

7.9.5 Уничтожение архивных документов

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

7.10 Смена ключей подписи доверенного лица УЦ

7.10.1 Плановая смена ключей доверенного лица УЦ

Плановая смена ключей подписи (ключа ЭП и соответствующего ему ключа проверки ЭП) доверенного лица (администратора) УЦ выполняется в соответствии со сроком действия сертификата доверенного лица УЦ.

Процедура плановой смены ключей подписи доверенного лица УЦ осуществляется в следующем порядке:

- доверенное лицо УЦ формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;

- доверенное лицо УЦ изготавливает сертификат нового ключа проверки ЭП и подписывает его ЭП с использованием нового ключа ЭП.

Старый ключ ЭП доверенного лица УЦ используется в течение своего срока действия для формирования списков аннулированных сертификатов, издаваемых УЦ в период действия старого ключа ЭП доверенного лица УЦ.

7.10.2 Внеплановая смена ключей подписи доверенного лица УЦ

Внеплановая смена ключей подписи выполняется в случае компрометации или угрозы компрометации ключа ЭП доверенного лица УЦ.

Процедура внеплановой смены ключей подписи доверенного лица УЦ выполняется в порядке, определенной процедурой плановой смены ключей подписи доверенного лица УЦ.

После выполнения процедуры внеплановой смены ключей подписи доверенного лица УЦ, сертификат доверенного лица УЦ аннулируется (отзывается) путем занесения в список аннулированных сертификатов.

8 СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

8.1 Структура сертификата, изготавливаемого УЦ в электронной форме

УЦ издает сертификаты пользователей УЦ и доверенного лица (администратора) УЦ в электронной форме, которая определена стандартом X.509 в соответствии с RFC 4491.

8.1.1 Базовые поля сертификата

Сертификаты ключей подписи содержат следующие базовые поля X.509:

- Signature: ЭП доверенного лица УЦ
- Issuer: Идентифицирующие данные УЦ
- Validity: Даты начала и окончания срока действия сертификата
- Subject: Идентифицирующие данные владельца сертификата

- SubjectPublicKeyInformation: Идентификатор алгоритма средств ЭП, с которыми используется данный ключ проверки ЭП, значение ключа проверки ЭП.
  Значение ключа проверки ЭП владельца сертификата, а также идентификатор криптографического алгоритма, с которым должен использоваться данный ключ
- Version: Версия сертификата формата X.509
- SerialNumber: Уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов УЦ

Требования к сертификату устанавливают необходимость использования дополнительных атрибутов Subject:

- ОГРН владельца сертификата − юридического лица;
- СНИЛС владельца сертификата − физического лица;
- ИНН владельца сертификата.

8.1.2 Дополнения сертификата

Сертификаты ключей подписи содержат следующие дополнения:

- subjectAlternativeName Альтернативное имя субъекта
- AuthorityKeyIdentifier: Идентификатор ключа проверки ЭП доверенного лица УЦ
- SubjectKeyIdentifier: Идентификатор ключа ЭП владельца сертификата
- ExtendedKeyUsage: Область (области) использования ключа ЭП, при которой(-ых) электронный документ с ЭП будет иметь юридическое значение
- CRLDistributionPoint: Точка распространения списка аннулированных сертификатов, изданных УЦ (может включаться или нет в соответствии с настройками УЦ)
- KeyUsage: Назначение ключа ЭП
- Basic Constraints: Определяет принадлежность сертификата Удостоверяющему центру и ограничение длины цепочки сертификатов для подчиненного УЦ.

Требования к сертификату проверки ЭП устанавливают необходимость использования следующих дополнений:

- certificatePolicies: Предназначено для обозначения политик сертификации, в соответствии с которыми должен использоваться квалифицированный сертификат
- subjectSignTool: Для указания в квалифицированном сертификате наименования используемого владельцем квалифицированного сертификата средства ЭП
- IssuerSignTool: Для указания в квалифицированном сертификате наименования средств ЭП и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством Российской Федерации

8.1.3 Поддерживаемые параметры и идентификаторы алгоритмов

УЦ обеспечивает формирование ключей подписи пользователей в соответствии с параметрами:

- Алгоритм подписи: ГОСТ Р 34.10-2001
- Описание: Стандарт ЭП, основанный на арифметике эллиптических кривых. OID «1.2.643.2.2.19»
- Параметры ключа проверки ЭП: ГОСТ Р 34.10-2001 Параметры по умолчанию
  ГОСТ Р 34.10-2001 «Оскар»
  ГОСТ Р 34.10-2001 Параметры подписи С
- Параметры подписи: Набор параметров по умолчанию (рекомендуется).
  OID «1.2.643.2.2. 35.1»
  Набор параметров B
  OID «1.2.643.2.2. 35.2»
  Набор параметров C
  OID «1.2.643.2.2. 35.3»
- Длина ключа: 512
- Алгоритм подписи ГОСТ Р 34.10-2012/1024

- Описание — Стандарт ЭП, основанный на арифметике эллиптических кривых. OID «1.2.643.7.1.1.1.2»
- Параметры ключа проверки ЭП: — ГОСТ Р 34.10-2012 Параметры А
  ГОСТ Р 34.10-2012 Параметры В
- Параметры подписи: — Набор параметров «ТК 26» (Параметры А) (рекомендуется)
  OID «1.2.643.7.1.2.1.2.1»
  Набор параметров «ТК 26» (Параметры В)
  OID «1.2.643.7.1.2.1.2.2»
- Длина ключа: — 1024

8.1.4 Формы имени

В сертификате поля идентификационных данных доверенного лица УЦ и владельца сертификата содержат атрибуты имени формата X.500.

8.1.5 Ограничения на имена

Обязательными атрибутами поля идентификационных данных доверенного лица УЦ центра являются:

- Common Name: — Фамилия, имя, отчество для физического лица. Наименование организации, являющейся владельцем УЦ, для юридического лица.
- Organization: — Наименование организации, являющейся владельцем УЦ
- Organization Unit: — Наименование подразделения, сотрудником которого является доверенное лицо УЦ
- INN: — ИНН УЦ
- OGRN: — ОГРН владельца сертификата − юридического лица
- Country: — RU
- State: — Субъект Российской федерации, где зарегистрирована организация, являющейся владельцем УЦ

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

- Common Name: — Фамилия, имя, отчество
- SNILS: — СНИЛС владельца сертификата − физического лица
- Country: — RU

- Surname Фамилия владельца сертификата
- Given Name Имя и отчество владельца сертификата

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

- Common Name: Наименование организации, которую представляет владелец сертификата.
- SNILS: СНИЛС представителя организации
- Surname Фамилия представителя организации, являющейся владельцем сертификата
- Given Name Имя и отчество представителя организации, являющейся владельцем сертификата
- Organization: Наименование организации, которую представляет владелец сертификата
- Organization Unit: Наименование подразделения организации, сотрудником которого является владелец сертификата
- Title Должность представителя организации
- INN: ИНН владельца сертификата − юридического лица
- OGRN: ОГРН владельца сертификата − юридического лица
- Country: RU
- State: Субъект Российской Федерации, где зарегистрирована организация, которую представляет владелец сертификата

Обязательными атрибутами поля идентификационных данных владельца сертификата ключа подписи, являющегося юридическим лицом, являются:

- Common Name: Наименование организации, которая является владельцем сертификата.
- Organization: Наименование организации
- INN: ИНН владельца сертификата − юридического лица
- OGRN: ОГРН владельца сертификата − юридического лица
- Country: RU

- State: Субъект Российской Федерации, где зарегистрирована организация, которую представляет владелец сертификата

Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося индивидуальным предпринимателем, являются:

- Common Name: Фамилия, имя, отчество.
- Organization: Наименование индивидуального предпринимателя, которого представляет владелец сертификата
- INN: ИНН индивидуального предпринимателя
- E-mail: Адрес электронной почты
- Country: RU
- State: Субъект Российской Федерации, где зарегистрирована организация, которую представляет владелец сертификата
- Surname Фамилия владельца сертификата
- Given Name Имя и отчество владельца сертификата
- OGRNIP ОГРН индивидуального предпринимателя

8.2 Структура CRL, изготавливаемого УЦ в электронной форме

УЦ издает списки аннулированных сертификатов пользователей УЦ и доверенного лица УЦ в электронной форме (далее по тексту раздела – CRL) формата X.509.

8.2.1 Дополнения CRL

- AuthorityKeyIdentifier: Идентификатор ключа проверки ЭП доверенного лица УЦ
- ReasonCode: Код причины отзыва сертификата ключа проверки ЭП

9 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

9.1 Инженерно-технические меры защиты информации

9.1.1 Размещение технических средств УЦ

Серверы и телекоммуникационное оборудование размещаются в выделенном помещении (далее по тексту – серверное помещение).

Серверы и телекоммуникационное оборудование размещаются в шкафу-стойке (cabinet).

Остальные технические средства УЦ размещаются в рабочих помещениях УЦ по схеме организации рабочих мест персонала.

9.1.2 Контроль защищенности вычислительной техники

Технические средства УЦ включают следующую функциональность:

- контроль доступа к сервисам УЦ и ролям УЦ;
- идентификация и аутентификация соответствующих Администраторов;
- криптографическая защита передаваемых сообщений и базы данных;
- архивирование данных пользователей и аудита УЦ;
- аудит событий, относящихся к обеспечению безопасности;
- механизмы резервного копирования и восстановления системы УЦ.

Данная функциональность предоставляется средствами ОС и комбинацией средств ОС, ПО УЦ, СЗИ и физических средств обеспечения безопасности.

Совместно с ViPNet УЦ используются криптосредства соответствующие требованиям ФСБ России к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну по классу КС2 или КС3 (в зависимости от варианта исполнения ViPNet УЦ).

9.1.3 Физический доступ

Серверное помещение УЦ оборудовано системой контроля доступа с идентификацией по карте.

Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

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

Идентификационные карты для доступа в серверное помещение выдаются сотрудникам УЦ по приказу руководителя УЦ.

Ключи механических замков рабочих помещений УЦ выдаются сотрудникам УЦ по распоряжению руководителя УЦ согласно схеме организации рабочих мест персонала.

Контроль целостности программных и технических средств УЦ осуществляется при каждой загрузке средств УЦ, также встроены механизмы периодического (раз в 24 часа) тестирования целостности ПО. Не реже чем один раз в сутки должна осуществляться перезагрузка всех средств УЦ.

9.1.4 Электроснабжение и кондиционирование воздуха

Технические средства УЦ подключены к общегородской сети электроснабжения.

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

Серверы, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение 8 часов после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников УЦ, 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 УЦ, используемые для архивного хранения документов на бумажных и съемных магнитных носителях, оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения УЦ оборудованы средствами вентиляции и кондиционирования воздуха согласно санитарно-гигиеническими нормами СНиП.

9.1.5 Подверженность воздействию влаги

Защита серверов и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке (cabinet).

9.1.6 Предупреждение и защита от возгорания

Серверное помещение УЦ оборудовано системой автоматического пожаротушения, пожарной сигнализацией и дымоудаления. Пожарная безопасность помещений УЦ обеспечивается согласно нормами и требованиями СНиП по классу Ф3.5.

9.1.7 Хранение документированной информации

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

9.1.8 Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками УЦ, которые обеспечивают документирование.

9.2 Организационные меры защиты информации

9.2.1 Предъявляемые требования к персоналу УЦ

У доверенного лица (администратора) УЦ должно быть высшее профессиональное образование и профессиональная подготовка в области информационной безопасности, стаж работы в этой области должен составлять более 2 лет.

9.2.2 Профессиональная переподготовка и повышение квалификации персонала

Профессиональной переподготовки персонала УЦ не требуется.

Повышение квалификации в областях знаний, согласно занимаемым должностям, сотрудникам УЦ необходимо осуществлять не реже одного раза в 2 года.

9.2.3 Организация сменной работы

Деятельность УЦ 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 будние дни.

Выходными днями являются: суббота, воскресенье, а также дни общенациональных праздников.

9.2.4 Организация доступа персонала к документам и документации

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

9.2.5 Охрана здания и помещений

УЦ должен иметь собственную (привлекаемую) службу охраны здания и помещений, обеспечивающую:

- обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) УЦ;
- сохранность материальных ценностей и документов;
- предупреждение происшествий и ликвидацию их последствий.

9.3 Юридические меры защиты информации

УЦ должен иметь разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг (см. раздел [2.2] настоящего Регламента).

Системы безопасности УЦ и защиты информации должны быть созданы и поддерживаться на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с законодательством Российской Федерации.

Все меры по защите информации на УЦ должны быть введены в действие приказами руководителя УЦ.

Для обеспечения деятельности УЦ необходимо использовать сертифицированные средства ЭП и криптографической защиты информации.

Исключительные имущественные права на информационные ресурсы УЦ должны находиться в собственности УЦ.

Пользователям УЦ необходимо предоставить неисключительные имущественные права на сертификаты и списки аннулированных сертификатов, изготавливаемых УЦ в объеме прав согласно разделу [3.2] настоящего Регламента.

ПРИЛОЖЕНИЕ 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Доверенное лицо

Лицо, которое удостоверяющий центр наделил полномочиями по созданию и выдаче сертификатов ключей проверки ЭП от имени УЦ, подписываемых ЭП, основанной на сертификате ключа проверки ЭП, выданном доверенному лицу этим УЦ.

Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата ключа проверки ЭП.

Запрос на отзыв сертификата

Сообщение, содержащее необходимую информацию для отзыва сертификата ключа проверки ЭП.

Заявитель

Лицо, обратившееся за получением сертификата ключа проверки ЭП. С момента выдачи сертификата удостоверяющим центром Заявитель становится владельцем сертификата (пользователем УЦ).

Идентификация

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

Ключ проверки ЭП

Уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

Ключ ЭП

Уникальная последовательность символов, предназначенная для создания ЭП.

Ключевой носитель

Носитель, содержащий один или несколько ключей.

Компрометация ключа

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

Плановая смена ключей

Смена ключей с установленной в системе периодичностью.

Пользователь УЦ (владелец сертификата)

Лицо, которому Удостоверяющим центром выдан сертификат ключа проверки электронной подписи.

Сертификат (сертификат ключа проверки ЭП)

Электронный документ или документ на бумажном носителе, выданный УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Требования к полям сертификата проверки ЭП определены в приказе ФСБ от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Список аннулированных сертификатов (CRL)

Созданный УЦ список сертификатов ключей проверки ЭП, аннулированных до окончания срока их действия.

Средства ЭП

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

СПИСОК ЛИТЕРАТУРЫ

1. «Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».
2. ISO/IEC 9594-8:2008. «Информационные технологии. Взаимосвязь открытых систем. Директория. Структура сертификата на общий ключ и атрибуты».
3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
4. Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».
5. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					