УТВЕРЖДЕН

ФРКЕ.00114-05 90 02-ЛУ

Программный комплекс

«ViPNet Удостоверяющий центр 4 (версия 4.6)»

Типовой регламент функционирования

ФРКЕ.00114-05 90 02

2016

Аннотация

Настоящий документ содержит типовой Регламент удостоверяющего центра (далее – УЦ) организации, эксплуатирующей программный комплекс ViPNet Удостоверяющий центр 4 (версия 4.6) (далее – ПК ViPNet УЦ).

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

Регламент УЦ 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) https://tools.ietf.org/html/rfc3647.

Информация о разработчике ПК ViPNet УЦ:

ОАО «ИнфоТеКС»

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

Телефон: (495) 737-61-92

Факс (495) 737-72-78

http://www.infotecs.ru

Содержание

Термины и определения 7
Перечень сокращений 9
1 Введение 10
1.1 Обзорная информация 10
1.2 Идентификация Регламента 10
1.3 Публикация Регламента 10
1.4 Область применения Регламента 10
1.5 Срок действия Регламента 11
1.6 Контактная информация 11
2 Общие положения 12
2.1 Функции УЦ 12
2.2 Услуги, предоставляемые УЦ 12
2.3 Разграничение полномочий в УЦ 13
2.3.1 Группа администраторов средств УЦ 13
2.4 Разрешение споров 16
2.5 Платность услуг 16
2.6 Ответственность 16
2.7 Прекращение деятельности 17
2.8 Порядок утверждения и внесения изменений в Регламент 17
3 Права 18
3.1 Права УЦ 18
3.2 Права пользователей УЦ 18
4 Обязанности 19
4.1 Обязанности УЦ 19
4.1.1 Аудит 19
4.1.2 Изготовление ключа ЭП и сертификата доверенного лица УЦ 19
4.1.3 Синхронизация времени 19
4.1.4 Регистрация пользователей УЦ 19
4.1.5 Изготовление ключей ЭП и ключей проверки ЭП пользователей УЦ 19
4.1.6 Изготовление сертификатов 20
4.1.7 Аннулирование сертификатов 20
4.1.8 Уведомления 20
4.1.9 Ведение реестра сертификатов 20

4.1.10 Прочие обязанности 21
4.2 Обязанности пользователей УЦ 21
4.2.1 Обязанности лиц, проходящих процедуру регистрации в УЦ 21
4.2.2 Обязанности пользователей УЦ 21
5 Политика конфиденциальности 22
5.1 Типы информации конфиденциального характера 22
5.2 Типы информации УЦ, не являющейся конфиденциальной 22
5.3 Исключительные полномочия УЦ 22
6 Процедуры и механизмы 23
6.1 Сценарии взаимодействия пользователей с УЦ 23
6.2 Процедура регистрации пользователей УЦ 23
6.2.1 Заявление на регистрацию 23
6.2.2 Идентификация пользователя УЦ 25
6.2.3 Регистрация пользователя УЦ, обработка запроса на издание сертификата 25
6.3 Идентификация зарегистрированного пользователя 26
6.4 Аутентификация зарегистрированного пользователя 26
6.4.1 Очная аутентификация зарегистрированного пользователя 26
6.4.2 Аутентификация зарегистрированного пользователя по сертификату 26
6.5 Изготовление пары ключей ЭП 26
6.5.1 Заявление на изготовление пары ключей ЭП 27
6.5.2 Изготовление и выдача пары ключей ЭП владельцу 27
6.6 Изготовление сертификата и предоставление его владельцу 27
6.6.1 Заявление и запрос на изготовление сертификата 28
6.6.2 Идентификация владельца сертификата 29
6.7 Аннулирование сертификата 29
6.7.1 Заявление на аннулирование сертификата 29
6.7.2 Протоколы аннулирования сертификатов 30
6.8 Проверка сертификата по заявлению пользователя 30
6.9 Срок хранения сертификата 31
6.10 Процедура подтверждения ЭП с использованием сертификата 31
6.11 Механизм доказательства обладания ключом ЭП 31
6.12 Проверка уникальности пары ключей ЭП 31
7 Дополнительные положения 33
7.1 Идентифицирующие данные доверенного лица УЦ 33

7.2 Сроки действия ключей ЭП доверенного лица УЦ 33
7.3 Требования к средствам ЭП 33
7.4 Сроки действия ключей ЭП и сертификатов пользователей 34
7.5 Назначение пары ключей ЭП и сертификата 34
7.6 Меры защиты ключей ЭП 34
7.7 Сертификат в электронной форме 35
7.8 Сертификат на бумажном носителе 35
7.9 Архивное хранение документированной информации 36
7.9.1 Состав архивируемых документов 36
7.9.2 Источник комплектования архивного фонда 36
7.9.3 Архивохранилище 36
7.9.4 Срок архивного хранения 36
7.9.5 Уничтожение архивных документов 36
7.10 Смена пары ключей ЭП доверенного лица УЦ 37
7.10.1 Плановая и внеплановая смена пары ключей ЭП доверенного лица УЦ 37
8 Структуры сертификатов и CRL 38
8.1 Структура сертификата, изготавливаемого УЦ в электронной форме 38
8.1.1 Базовые поля сертификата 38
8.1.2 Дополнения сертификата 38
8.1.3 Поддерживаемые параметры и идентификаторы алгоритмов 39
8.1.4 Формы имени 40
8.1.5 Ограничения на имена 40
8.2 Структура списка аннулированных сертификатов, изготавливаемого УЦ в электронной форме 42
8.2.1 Дополнения списка аннулированного сертификата 42
9 Обеспечение безопасности 43
9.1 Инженерно-технические меры защиты информации 43
9.1.1 Размещение технических средств УЦ 43
9.1.2 Контроль защищенности вычислительной техники 43
9.1.3 Физический доступ 44
9.1.4 Электроснабжение и кондиционирование воздуха 44
9.1.5 Подверженность воздействию влаги 45
9.1.6 Предупреждение и защита от возгорания 45
9.1.7 Хранение документированной информации 45

9.1.8 Уничтожение документированной информации 45
9.2 Организационные меры защиты информации 45
9.2.1 Предъявляемые требования к персоналу УЦ 45
9.2.2 Профессиональная переподготовка и повышение квалификации персонала 45
9.2.3 Организация сменной работы 46
9.2.4 Организация доступа персонала к документам и документации 46
9.2.5 Охрана здания и помещений 46
9.3 Юридические меры защиты информации 46
Список используемой литературы 48

Термины и определения

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности пользователя УЦ.

Доверенное лицо – лицо, которое УЦ наделил полномочиями по созданию и выдаче сертификатов от имени УЦ, подписываемых ЭП, основанной на сертификате, выданном доверенному лицу этим УЦ.

Запрос на сертификат – сообщение, содержащее необходимую информацию для получения сертификата.

Запрос на аннулирование сертификата – сообщение, содержащее необходимую информацию для аннулирования сертификата.

Заявитель – лицо, обратившееся за получением сертификата ключа проверки ЭП. С момента выдачи сертификата УЦ 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 УЦ выдан сертификат ключа проверки ЭП.

Сертификат ключа проверки ЭП (сертификат) – электронный документ или документ на бумажном носителе, выданный УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата.

Требования к полям квалифицированного сертификата ключа 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, 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.

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 от 06.04.2011 № 63-ФЗ «Об электронной подписи».

ViPNet – торговая марка программных продуктов компании «ИнфоТеКС».

Перечень сокращений

CRL	–	список аннулированных сертификатов
ИНН	–	идентификационный номер налогоплательщика
ИП	–	индивидуальный предприниматель
НСД	–	несанкционированный доступ
ОГРН	–	основной государственный регистрационный номер
ОГРНИП	–	основной государственный регистрационный номер индивидуального предпринимателя
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СНИЛС	–	страховой номер индивидуального лицевого счета
УКЦ	–	Удостоверяющий и ключевой центр
УЦ	–	Удостоверяющий центр
ЦР	–	Центр регистрации
ЭП	–	электронная подпись

1 Введение

1.1 Обзорная информация

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг УЦ _____(полное наименование юридического лица или индивидуального предпринимателя), включая обязанности пользователей УЦ и членов группы администраторов УЦ, 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 (версия 4.6)». Типовой регламент функционирования»».

Индекс:

Дата: ___.___.20___г.

Объектный идентификатор: _____.

1.3 Публикация Регламента

Настоящий Регламент распространяется:

1 В электронной форме:
   - из репозитория УЦ по адресу _____ (URL с указанием протокола);
   - через e-mail от отправителя _____ (адрес электронной почты отправителя).

2 В бумажной форме:
   - 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 (далее – ЭП) УЦ к файлу электронного образа Регламента.

1.4 Область применения Регламента

Настоящий Регламент предназначен служить средством официального уведомления и информирования всех заинтересованных сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ, а также соглашением, налагающим обязанности на все вовлеченные в эти взаимоотношения стороны.

1.5 Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента – 6 лет.

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

Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе «Публикация Регламента».

1.6 Контактная информация

_____ (полное наименование юридического лица или индивидуального предпринимателя).

_____ (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 УЦ

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

- издает сертификаты ключей проверки электронных подписей (далее − сертификат) и выдает такие сертификаты лицам, обратившимся за их получением (далее − заявитель);
- устанавливает сроки действия сертификатов;
- аннулирует изданные этим УЦ 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 изданных и аннулированных этим УЦ сертификатов (далее – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим УЦ сертификатах, а также сведения о датах прекращения действия или аннулирования сертификатов и основаниях;
- 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 УЦ

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

- внесение в реестр УЦ регистрационной информации о владельцах сертификатов;
- изготовление сертификатов в электронной форме;
- изготовление сертификатов на бумажном носителе;
- формирование ключей ЭП и ключей проверки ЭП по обращениям заявителей с записью их на ключевой носитель;

- ведение реестра сертификатов, изданных в данном УЦ;
- предоставление в электронной форме сертификатов, находящихся в реестре изготовленных сертификатов, по запросам пользователей;
- аннулирование сертификатов по обращениям владельцев сертификатов;
- ведение списков аннулированных сертификатов (далее – CRL) и предоставление доступа к ним пользователям;
- подтверждение подлинности ЭП в документах, представленных в электронной форме, по обращениям пользователей;
- подтверждение подлинности ЭП доверенного лица УЦ в изготовленных им сертификатах по обращениям пользователей;
- распространение средств ЭП по обращениям пользователей.

2.3 Разграничение полномочий в УЦ

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». Данную роль исполняет администратор УКЦ (ViPNet Удостоверяющий и ключевой центр, входящий в состав ПК ViPNet Administrator);
- роль «администратор Центра регистрации». Данную роль исполняет группа администраторов Центра регистрации (ViPNet Registration Point);
- роль «администратор Сервиса публикации». Данную роль исполняет группа администраторов Сервиса публикации (ViPNet Publication Service);

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 ПК ViPNet УЦ в целом;
- обеспечивает синхронизацию времени на серверах времени и контроль синхронизации времени на компьютерах пользователей УЦ;

- осуществляет контроль над соблюдением правил эксплуатации и соблюдением мер защиты от несанкционированного доступа (далее – НСД);
- осуществляет проверку целостности программного обеспечения (далее – ПО компонентов ПК ViPNet УЦ;
- осуществляет аудит событий по журналам компонентов ПК ViPNet УЦ, журналам операционной системы (далее – ОС) 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 ПК ViPNet УЦ;
- создание и поддержка профилей членов групп администраторов;
- конфигурация профиля и параметров журнала аудита;
- осуществление настройки ОС и прикладного ПО.

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

2.3.1.3 Администратор УКЦ

Администратор УКЦ исполняет роль администратора сертификации с основными обязанностями: создание и аннулирование сертификатов.

Администратор УКЦ выполняет следующие функции:

- обеспечивает создание ключей ЭП, ключей проверки ЭП, ключей шифрования;
- осуществляет проверку однородности[1];
- осуществляет издание сертификатов по запросам на издание или обновление;
- осуществляет проведение работ по аннулированию, приостановлению и возобновлению действия сертификатов;
- по обращениям заявителей осуществляет проверку ЭП в электронных документах и проверку ЭП в сертификате;

[1] Под однородностью понимается соответствие алгоритма ЭП, указанного в запросе на сертификат заявителя алгоритму ключа ЭП администратора УКЦ.

- при необходимости осуществляет настройку службы информирования (ViPNet CA Informing);
- осуществляет своевременное создание архивов баз данных и восстановление их при сбоях;
- осуществляет настройку журналов в ПО ViPNet Удостоверяющий и ключевой центр (далее – ViPNet УКЦ);
- осуществляет ведение документации УЦ согласно должностным инструкциям сотрудников УЦ;
- осуществляет рассылку уведомлений о событиях, связанных с сертификатами, изданными данным УЦ, формирование отчетов, позволяющих предоставлять информацию о сертификатах.

Для обеспечения своих функций администратор УКЦ должен:

- быть зарегистрирован на сетевом узле (далее – СУ), на котором установлена программа ViPNet УКЦ;
- 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 Центра регистрации (далее – ЦР) выполняет следующие функции:

- осуществляет регистрацию пользователей;
- осуществляет проверку соответствия алгоритма ключа проверки ЭП, заданного в запросе на сертификат пользователя, алгоритму ЭП собственного ключа администратора ЦР;
- создает запросы на издание, обновление и аннулирование сертификатов;
- осуществляет проверку и выдачу сертификатов;
- осуществляет настройку интерфейса для автоматизированной обработки и передачи в УЦ запросов на издание сертификатов.

Для обеспечения своих функций администратор ЦР должен:

- быть зарегистрирован на СУ, на котором установлена программа ViPNet Registration Point;
- иметь действительный ключ ЭП и сертификат для ЭП 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.

2.3.1.5 Группа администраторов Сервиса публикации

Администратор Сервиса публикации выполняет следующие функции:

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

Для обеспечения своих функций администратор Сервиса публикации должен:

- быть зарегистрирован на СУ, на котором установлена программа 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 УЦ и пользователь УЦ.

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

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде.

2.5 Платность услуг

Услуга УЦ по предоставлению CRL 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

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

Претензии к УЦ ограничиваются указанием на несоответствие его действий настоящему Регламенту.

2.7 Прекращение деятельности

Деятельность УЦ 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 УЦ.

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

3 Права

3.1 Права УЦ

УЦ имеет право:

- предоставлять в электронной форме сертификаты, находящиеся в реестре УЦ, всем лицам, обратившимся в УЦ;
- отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на регистрацию без предоставления информации о причинах отказа;
- отказать в изготовлении 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 в случае установленного факта компрометации соответствующего ключа ЭП с уведомлением владельца аннулированного сертификата и указанием обоснованных причин.

3.2 Права пользователей УЦ

Пользователи УЦ имеют следующие права:

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

4 Обязанности

4.1 Обязанности УЦ

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 и сертификата доверенного лица УЦ

УЦ обязан формировать ключи ЭП и издавать сертификат для доверенного лица.

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

Доверенное лицо не может использовать несколько пар ключей и сертификатов, даже в том случае, если они у него есть в наличии и срок действия их не истек. Для подписи издаваемых сертификатов он должен использовать только одну пару ключей и сертификат с самой поздней датой издания. Остальные ключи и сертификаты он может использовать только для подписи CRL. 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 УЦ.

4.1.4 Регистрация пользователей УЦ

УЦ обеспечивает регистрацию пользователей УЦ по заявлениям на регистрацию.

УЦ не имеет права разглашать (публиковать) регистрационную информацию пользователей, 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 по его заявлению.

УЦ обязан обеспечить сохранение в тайне изготовленного ключа ЭП пользователя.

4.1.6 Изготовление сертификатов

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

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 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 CRL.

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 CRL.

Временем опубликования CRL признается включенное в CRL время его изготовления.

УЦ обязан включать полный адрес (URL) CRL в издаваемые сертификаты.

4.1.9 Ведение реестра сертификатов

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

Реестр сертификатов ведется в электронном виде.

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

4.1.10 Прочие обязанности

УЦ обязан уведомлять владельца сертификата о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования ключа ЭП и сертификата.

4.2 Обязанности пользователей УЦ

4.2.1 Обязанности лиц, проходящих процедуру регистрации в УЦ

Лица, проходящие процедуру регистрации в 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 УКЦ);
- не использовать ключ ЭП, связанный с сертификатом, который аннулирован, действие которого прекращено или приостановлено;
- использовать для создания и проверки ЭП, создания ключей ЭП и ключей проверки ЭП только средства ЭП, сертифицированные по требованиям ФСБ России.

5 Политика конфиденциальности

5.1 Типы информации конфиденциального характера

Ключ ЭП является информацией конфиденциального характера лица, являющегося владельцем соответствующего сертификата. УЦ не осуществляет хранение ключей ЭП пользователей УЦ.

Персональная и корпоративная информация о пользователях, не являющаяся частью сертификата, считается конфиденциальной.

5.2 Типы информации УЦ, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, является общедоступной.

Общедоступная информация может публиковаться по решению УЦ.

Место, способ и время публикации также определяется решением УЦ.

Информация, включаемая в сертификаты и CRL, издаваемые УЦ, не считается конфиденциальной.

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 УЦ

Возможны следующие сценарии получения ключей ЭП и сертификата в УЦ:

1 Пользователь самостоятельно формирует при помощи сертифицированного СКЗИ пару ключей и запрос на издание сертификата в формате PKCS#10 (https://tools.ietf.org/html/rfc2986) и приносит данный запрос в ЦР. Администратор ЦР проверяет запрос, регистрирует пользователя, подписывает запрос своим ключом и отправляет в программу ViPNet УКЦ, где администратор УКЦ 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 лично обращается с 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 программу ViPNet УКЦ. Администратор УКЦ 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:
  - идентификационный номер налогоплательщика (далее – ИНН) физического лица;
  - фамилию, имя и отчество;
  - страховой номер индивидуального лицевого счета владельца квалифицированного сертификата (далее – СНИЛС);
  - адрес электронной почты (e-mail);
- контактные телефоны.

Для физического лица, представляющего юридическое лицо:

- идентификационные данные, включающие:
  - наименование организации;
  - ИНН организации;
  - основной государственный регистрационный номер (далее – ОГРН) 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 (далее – ИП):

- идентификационные данные, включающие:
  - фамилию, имя и отчество;
  - адрес электронной почты (e-mail);
  - наименование ИП;
  - субъект Российской Федерации, в котором зарегистрирован ИП;
  - основной государственный регистрационный номер индивидуального предпринимателя (далее – ОГРНИП);
  - ИНН 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 ИП.

6.2.2 Идентификация пользователя УЦ

Идентификация пользователя выполняется в процессе его регистрации в ЦР 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 «Заявление на регистрацию»).

6.2.3 Регистрация пользователя УЦ, обработка запроса на издание сертификата

Регистрация пользователя УЦ осуществляется администратором ЦР 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 двух рабочих дней с момента поступления.

При принятии положительного решения осуществляется изготовление ключей ЭП и издание сертификата (см. раздел «Сценарии взаимодействия пользователей УЦ»).

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 осуществляется по идентификатору зарегистрированного пользователя, занесенному в реестр пользователей.

6.4 Аутентификация зарегистрированного пользователя

6.4.1 Очная аутентификация зарегистрированного пользователя

Очная аутентификация зарегистрированного пользователя 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. раздел «Процедура подтверждения ЭП с использованием сертификата).

6.5 Изготовление пары ключей ЭП

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

6.5.1 Заявление на изготовление пары ключей ЭП

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

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

Заявление на изготовление пары ключей ЭП рассматривается УЦ в течение трех рабочих дней с момента поступления.

6.5.2 Изготовление и выдача пары ключей ЭП владельцу

Изготовление пары ключей ЭП выполняется администратором ЦР на основании принятого заявления.

Изготовленная пара ключей ЭП записывается 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 изготовленную пару ключей ЭП, передается владельцу (заявителю). Факт выдачи ключей заносится в журнал учета изготовления и выдачи пары ключей ЭП 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. раздел «Заявление на изготовление пары ключей ЭП»).

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

Сертификаты, изданные в ViPNet УЦ, имеют структуру формата X.509 (RFC 4491 https://tools.ietf.org/html/rfc4491). Изданные квалифицированные сертификаты соответствуют требованиям, изложенным в приказе ФСБ России №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» и требованиям извещения об использовании стандартных атрибутов имени commonName (общее имя), surname (фамилия), givenName (приобретенное имя) и дополнительных

атрибутов имени поля «subject» в структуре квалифицированного сертификата ключа проверки электронной подписи.

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

После изготовления сертификата его владельцу направляется официальное уведомление (см. раздел «Уведомления»).

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 (CRL);
- 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:

- идентификационные данные пользователя (аналогично разделу 6.2.1 Заявление на регистрацию);
- текст запроса на сертификат;
- дата и подпись заявителя;

При необходимости предоставляется нотариальная доверенность.

При формировании запроса рекомендуется убедиться в однородности алгоритмов ЭП, т.е. в соответствии указанного в запросе на сертификат заявителя алгоритма ЭП алгоритму сертификата администратора ЦР.

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 ЭП, соответствующих ключам

проверки ЭП внутри запросов. Подпись подтверждает, что пользователь, передавший запрос, является обладателем пары ключей ЭП.

Запросы на сертификаты в формате SOK поступают в ViPNet УКЦ из ЦР. Запрос в формате SOK представляют хранилище сертификатов с объектом, имеющим структуру сертификата X.509. Запросы такого формата заверены сертификатом и подписаны ключом администратора ЦР. 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 «Структура сертификата, изготавливаемого УЦ в электронной форме»).

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 в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата указанием обоснованных причин аннулирования.

Администратор ЦР формирует запрос на аннулирование сертификата, подписывает его своим ключом и отправляет в ViPNet УКЦ, где запрос обрабатывается администратором УКЦ и сертификат попадет в CRL администратора УЦ (издателя сертификата) и будет иметь статус «Аннулирован». Данный CRL поступает администратору ЦР вместе с ответом на запрос об аннулировании сертификата. С момента получения остальными пользователями обновленного CRL аннулированный сертификат станет недействительным.

После аннулирования сертификата его владельцу направляется официальное уведомление (см. раздел «Уведомление о факте аннулирования сертификата»).

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 сертификата, который требуется аннулировать;
- причину аннулирования сертификата;
- дата и подпись заявителя.

6.7.2 Протоколы аннулирования сертификатов

В ViPNet УЦ информация об аннулированных сертификатах предоставляется пользователям путем предоставления CRL.

6.8 Проверка сертификата по заявлению пользователя

Проверка сертификата осуществляется УЦ по обращению пользователей на основании заявления в письменной форме, передаваемого заявителем в УЦ лично. Обязательным приложением к заявлению является цифровой носитель, содержащий сертификат (с расширением .cer), подвергающийся процедуре проверки. Срок рассмотрения заявления на подтверждение ЭП в сертификате составляет пять рабочих дней с момента поступления заявления в УЦ.

В случае ненадлежащего оформления заявления, отсутствия обязательных файлов или не подтверждения факта издания сертификата данным УЦ, УЦ имеет право отказать в проведении технической экспертизы. В таком случае заявителю возвращается заявление с соответствующей резолюцией уполномоченного лица УЦ.

Проверка сертификата заключается в подтверждении подлинности ЭП сертификата. Проверка производится администратором ЦР средствами ОС при проведении технической экспертизы. По результатам экспертизы предоставляется соответствующий протокол, подписанный собственноручной подписью администратора ЦР.

Перед началом проведения технической экспертизы администратор ЦР должен проверить цифровой носитель, предоставленный заявителем, с помощью используемого антивирусного средства.

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

Срок архивного хранения сертификата определен в разделе «Архивное хранение документированной информации».

6.10 Процедура подтверждения ЭП с использованием сертификата

Подтверждение ЭП в электронном документе осуществляется УЦ по обращению граждан (заявителей) в соответствии с порядком проверки ЭП, см. раздел «Проверка сертификата по заявлению пользователя».

6.11 Механизм доказательства обладания ключом ЭП

Заявления на изготовление сертификатов, поступающие в УЦ, должны содержать собственноручную подпись заявителя. При первом издании сертификата для данного пользователя пара ключей может быть сформирована непосредственно в ЦР. В этом случае факт обладания ключом ЭП подтверждается актом передачи пользователю ключевого носителя.

В случае если ключ ЭП формировался пользователем, в УЦ 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 УКЦ. Положительный результат проверки подписи средствами УЦ подтверждает, что заявитель является владельцем ключа ЭП, которому соответствует ключ проверки ЭП. В случае отсутствия подтверждения администратор УКЦ имеет право аннулировать изданный сертификат.

6.12 Проверка уникальности пары ключей ЭП

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 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.

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 (e-mail): _____
- субъект Российской Федерации: _____

7.2 Сроки действия ключей ЭП доверенного лица УЦ

Срок действия ключей ЭП доверенного лица (администратора) УКЦ составляет 3 года. При этом допускается использование ключа для подписи издаваемых сертификатов только в течение первых 15 месяцев с момента его издания. По истечении этого срока необходимо сформировать новый ключ ЭП и использовать его для подписания издаваемых сертификатов. При смене старый ключ ЭП не следует удалять, поскольку он будет использоваться для подписи CRL в течение трех лет с момента создания. Это необходимо для того, чтобы обеспечить возможность аннулирования пользовательских сертификатов.

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

В соответствии с требованиями приказа ФСБ России от 27 декабря 2011 года № 796 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 УКЦ составляет 16 лет.

До окончания трехлетнего срока с момента создания ключа ЭП администратора УКЦ, но после истечения срока действия ключа ЭП последнего сертификата пользователя, подписанного этим ключом, администратор УКЦ должен выпустить последний итоговый CRL. Срок действия итогового CRL должен быть ограничен сроком действия сертификата администратора УКЦ, соответствующего этому ключу ЭП.

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.

Средство ЭП должно обеспечивать выполнение мер защиты ключей ЭП (см. раздел «Меры защиты ключей ЭП»).

При использовании квалифицированных сертификатов средства ЭП должны быть сертифицированы в соответствии с Требованиями к средствам электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 года № 796.

7.4 Сроки действия ключей ЭП и сертификатов пользователей

Срок действия ключей ЭП пользователей УЦ не должен превышать 1 года и 3 месяцев.

Срок действия ключей проверки ЭП в соответствии с требованиями Приказа ФСБ РФ № 796 от 27 декабря 2011 года не должен превышать срок действия ключей ЭП более чем на 15 лет. Следовательно, максимально допустимый срок действия сертификата ключа проверки ЭП пользователя УЦ составляет 15 лет.

Срок действия сертификата устанавливается УЦ в момент его изготовления.

7.5 Назначение пары ключей ЭП и сертификата

Пара ключей 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, в случае их создания по заявлению пользователя в ЦР, должны записываться на ключевые носители. Допустимые ключевые носители указаны в документации на СКЗИ ViPNet CSP 4.2.

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

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

Если процедуру создания пары ключей ЭП пользователя УЦ выполняет администратор УКЦ, то он должен сообщить сформированный пароль владельцу ключей ЭП.

Ответственность за сохранение пароля в тайне возлагается на пользователя ключей ЭП.

Не допускается использовать одно и то же значение пароля для защиты нескольких ключей ЭП.

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

7.7 Сертификат в электронной форме

Сертификат в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту X.509, представленный в кодировке Der или Base64.

7.8 Сертификат на бумажном носителе

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

- серийный номер сертификата;
- срок действия сертификата;
- сведения о владельце сертификата (идентификационные данные владельца сертификата; ИНН, СНИЛС для владельца – физического лица; ИНН и ОГРН для владельца – юридического лица; ИНН и ОГРНИП для владельца – ИП 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 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 на бумажном носителе администратор УКЦ 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 подлежит следующая документированная информация:

- реестр сертификатов;
- сертификаты доверенного лица УЦ;
- журналы аудита средств ПК ViPNet УЦ;
- реестр зарегистрированных пользователей УЦ;
- заявления на изготовление ключей пользователей УЦ;
- заявления на изготовление сертификатов;
- 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 их уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников УЦ и назначаемой приказом руководителя УЦ.

7.10 Смена пары ключей ЭП доверенного лица УЦ

7.10.1 Плановая и внеплановая смена пары ключей ЭП доверенного лица УЦ

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

Процедура плановой смены пары ключей ЭП 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 CRL, издаваемых УЦ в период действия старого ключа ЭП доверенного лица УЦ.

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

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

Примечание. При наличии установленного доверия с другими УЦ, в том числе с УЦ Минкомсвязи России, после выполнения процедуры смены ключей ЭП доверенного лица УЦ необходимо повторно пройти процедуру установления доверия. При изменении используемых УЦ средств УЦ и/или средств ЭП для обеспечения возможности издания квалифицированных сертификатов также требуется провести смену ключей ЭП и повторить процедуру установления доверия с УЦ Минкомсвязи России.

8 Структуры сертификатов и CRL

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 https://tools.ietf.org/html/rfc4491.

8.1.1 Базовые поля сертификата

Сертификаты 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;
- ОГРНИП владельца сертификата.

8.1.2 Дополнения сертификата

Сертификаты 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 электронный документ с ЭП будет иметь юридическое значение;
- CRLDistributionPoint – точка распространения CRL, изданных УЦ (может включаться или нет, в соответствии с настройками УЦ);
- KeyUsage – назначение ключа ЭП;
- Basic Constraints – определяет принадлежность сертификата УЦ и ограничение длины цепочки сертификатов для подчиненного УЦ.

Требования к сертификату 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 пары ключей ЭП 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 бит;
- 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 бит.

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 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 или ИП;
- Country – RU (Россия);
- 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;
- INN – ИНН владельца сертификата − физического лица;
- Country – RU;
- Surname – фамилия владельца сертификата;
- Given Name – имя и отчество владельца сертификата.

Обязательными атрибутами поля идентификационных данных владельца сертификата, 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, 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 ИП, являются:

- Common Name – фамилия, имя, отчество;
- Organization – наименование ИП, которого представляет владелец сертификата;
- INN – ИНН ИП;

- 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 ИП.

8.2 Структура списка аннулированных сертификатов, изготавливаемого УЦ в электронной форме

УЦ издает CRL в электронной форме формата X.509.

8.2.1 Дополнения списка аннулированного сертификата

- AuthorityKeyIdentifier – идентификатор ключа проверки ЭП доверенного лица УЦ;
- ReasonCode – код причины аннулирования сертификата.

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 – 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, средствами защиты информации и физическими средствами обеспечения безопасности.

Совместно с ПК ViPNet УЦ используется (в зависимости от варианта исполнения ViPNet УЦ):

- СКЗИ ViPNet CSP 4.2 (исполнение 2), соответствующее требованиям ФСБ России к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и требованиям к средствам ЭП по классу КС2;
- СКЗИ ViPNet CSP 4.2 (исполнение 3), соответствующее требованиям ФСБ России к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну и требованиям к средствам ЭП, по классу КС3.

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

9.1.4 Электроснабжение и кондиционирование воздуха

Технические средства с установленными компонентами ПК ViPNet УЦ 4 подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые при эксплуатации ПК ViPNet УЦ 4, 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, обеспечивающим их работу в течение 8 часов после прекращения основного электроснабжения.

На технические средства, эксплуатируемые на рабочих местах с установленными компонентами ПК ViPNet УЦ, рекомендуется устанавливать источники бесперебойного питания.

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

Служебные помещения, 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 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 оборудовано системой автоматического пожаротушения и дымоудаления, пожарной сигнализацией. 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 УЦ должно быть высшее профессиональное образование и профессиональная подготовка в области информационной безопасности, стаж работы в этой области должен составлять более двух лет.

9.2.2 Профессиональная переподготовка и повышение квалификации персонала

Профессиональной переподготовки персонала УЦ не требуется.

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

9.2.3 Организация сменной работы

Деятельность УЦ по работе с пользователями УЦ в части приема заявлений в бумажной форме и изготовления сертификатов 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, связанным с предоставлением услуг (см. раздел «Услуги, предоставляемые УЦ»).

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 средства ЭП и СКЗИ ViPNet CSP 4.2, входящие в состав ПК ViPNet УЦ.

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

Пользователям УЦ необходимо предоставить неисключительные имущественные права на сертификаты и CRL, изготавливаемых УЦ в объеме прав согласно разделу «Права пользователей УЦ».

Список используемой 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					