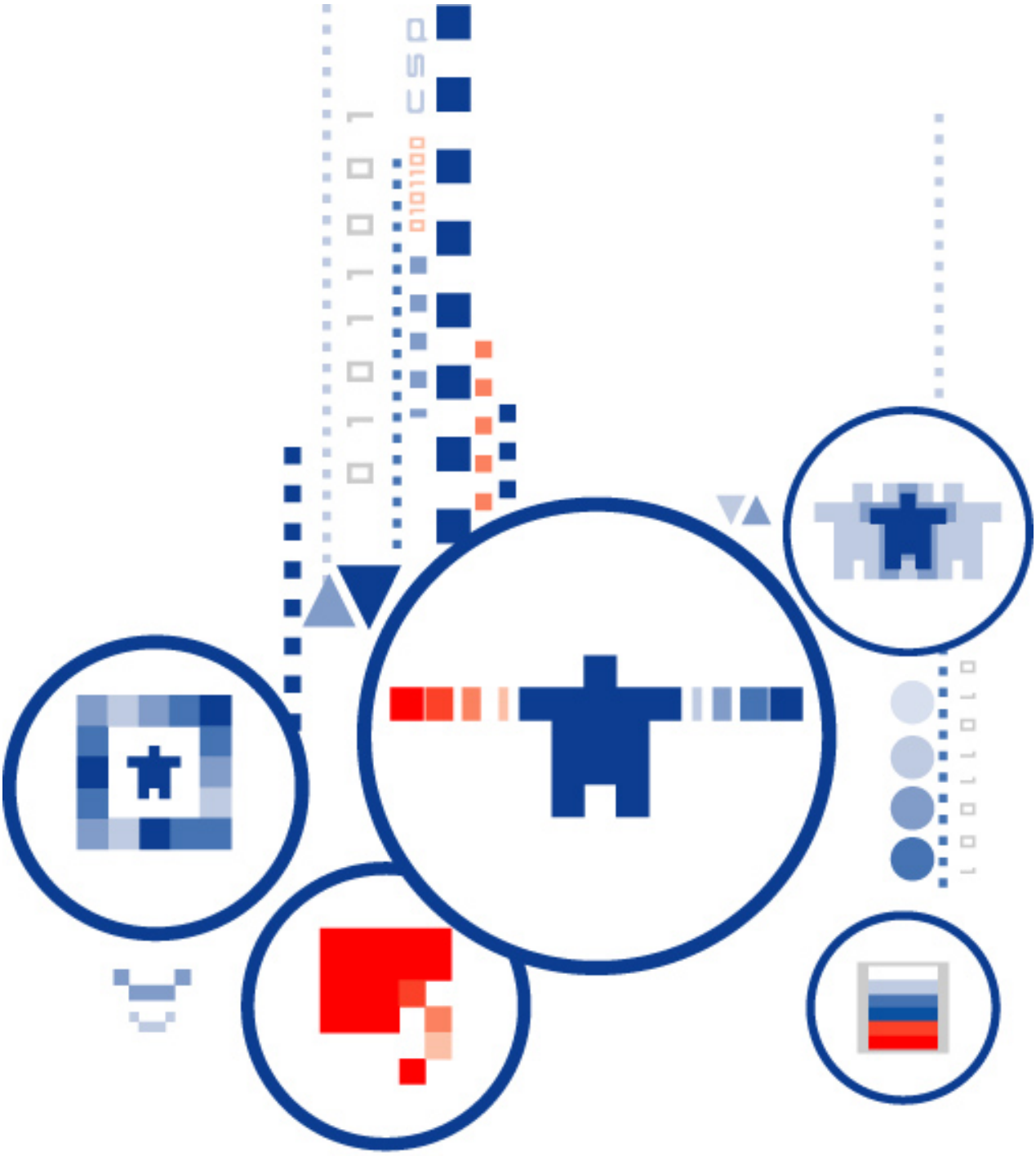
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 16-ЛУ

ЖТЯИ.00035-01 90 16



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Регламент

АННОТАЦИЯ

Настоящий документ содержит типовой Регламент удостоверяющего центра (УЦ) организации, эксплуатирующей программный комплекс «Удостоверяющий Центр «КриптоПро УЦ».

Деятельность удостоверяющего центра, в соответствии со статьей 8 Федерального закона № 1 от 10 января 2002 г. "Об электронной цифровой подписи", обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем (Договором) или соглашением участников этой системы, формой которого может быть Регламент эксплуатируемого УЦ.

Регламент удостоверяющего центра эксплуатирующей организации должен создаваться с учетом положений настоящего документа, действующего законодательства Российской Федерации, рекомендаций RFC 2527 (Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework).

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

127 018, Москва, улица Сущевский вал, 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Введение 7
1.1. Обзорная информация 7
1.2. Идентификация Регламента 7
1.3. Публикация Регламента 7
1.4. Область применения Регламента 7
1.5. Срок действия Регламента 7
1.6. Контактная информация 8
2. Общие положения 9
2.1. Назначение Удостоверяющего Центра 9
2.2. Услуги, предоставляемые Удостоверяющим Центром 9
2.3. Структура Удостоверяющего Центра 9
2.3.1. Административная служба УЦ 10
2.3.2. Служба Регистрации УЦ 10
2.3.3. Служба Безопасности УЦ 10
2.3.4. Техническая Служба УЦ 10
2.4. Пользователи услуг Удостоверяющего Центра 11
2.5. Разрешение споров 11
2.6. Платность услуг 11
2.7. Ответственность 12
2.8. Прекращение деятельности 12
2.9. Порядок утверждения и внесения изменений в Регламент 12
3. Права 13
3.1. Права Удостоверяющего Центра 13
3.2. Права пользователей УЦ 13
3.2.1. Пользователи Группы 1 13
3.2.2. Пользователи Группы 2 14
3.2.3. Пользователи Группы 3 14
3.2.4. Пользователи Группы 4 15
4. Обязательства 17
4.1. Обязательства Удостоверяющего Центра 17
4.1.1. Аудит 17
4.1.2. Ключ подписи уполномоченного лица Удостоверяющего Центра 17
4.1.3. Синхронизация времени 17
4.1.4. Регистрация пользователей УЦ 17
4.1.5. Изготовление закрытых и открытых ключей пользователей УЦ 17
4.1.6. Изготовление сертификатов открытых ключей 18
4.1.7. Аннулирование (отзыв) сертификатов открытых ключей 18
4.1.8. Приостановление действия сертификатов открытых ключей 18
4.1.9. Возобновление действия сертификатов открытых ключей 18
4.1.10. Уведомления 18
4.1.11. Реестр сертификатов открытых ключей 19
4.1.12. Прочие обязательства 20
4.2. Обязательства пользователей УЦ 20
4.2.1. Обязанности лиц, проходящих процедуру регистрации 20
4.2.2. Обязанности владельцев закрытых ключей 20
4.2.3. Обязанности владельца сертификата открытого ключа 20

4.2.4. Обязанности пользователей сертификатов открытых ключей 20
5. Политика конфиденциальности 21
5.1. Типы конфиденциальной информации 21
5.2. Типы информации, не являющейся конфиденциальной 21
5.3. Исключительные полномочия официальных лиц 21
6. Процедуры и механизмы 22
6.1. Процедура регистрации пользователей УЦ 22
6.1.1. Заявление на регистрацию 22
6.1.2. Идентификация пользователя УЦ 22
6.1.3. Регистрация пользователя УЦ в централизованном режиме 23
6.1.4. Регистрация пользователя УЦ в распределенном режиме 23
6.2. Идентификация зарегистрированного пользователя 25
6.3. Аутентификация зарегистрированного пользователя 25
6.3.1. Очная аутентификация зарегистрированного пользователя 25
6.3.2. Удаленная аутентификация зарегистрированного пользователя 25
6.3.3. Аутентификация зарегистрированного пользователя по сертификату открытого ключа 25
6.3.4. Аутентификация зарегистрированного пользователя по паролю 26
6.4. Изготовление ключей 26
6.4.1. Заявление на изготовление ключей 26
6.4.2. Изготовление и выдача ключей владельцу 26
6.5. Изготовление сертификата открытого ключа и предоставление его владельцу. 26
6.5.1. Заявление на изготовление сертификата открытого ключа в электронной форме 27
6.5.2. Заявление на изготовление сертификата открытого ключа в бумажной форме 27
6.5.3. Идентификация владельца сертификата открытого ключа 27
6.6. Аннулирование (отзыв) сертификата открытого ключа 27
6.6.1. Заявление на отзыв сертификата открытого ключа в электронной форме 28
6.6.2. Заявление на отзыв сертификата открытого ключа в бумажной форме 28
6.7. Приостановление действия сертификата открытого ключа 28
6.7.1. Заявление на приостановление действия сертификата открытого ключа в электронной форме 29
6.7.2. Заявление на приостановление действия сертификата открытого ключа в бумажной форме 29
6.7.3. Заявление на приостановление действия сертификата открытого ключа в устной форме 29
6.8. Возобновление действия сертификата открытого ключа 30
6.8.1. Заявление на возобновление действия сертификата открытого ключа в электронной форме 30
6.8.2. Заявление на возобновление действия сертификата открытого ключа в бумажной форме 30
6.9. Срок хранения сертификата открытого ключа 31
6.10. Процедура подтверждения электронной цифровой подписи с использованием сертификата открытого ключа 31
6.11. Процедура подтверждения электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификате открытого ключа 32

6.12. Механизм доказательства обладания закрытым ключом, соответствующим открытому ключу 33
7. Дополнительные положения 34
7.1. Идентифицирующие данные уполномоченного лица Удостоверяющего Центра 34
7.2. Сроки действия ключей уполномоченного лица Удостоверяющего Центра 34
7.3. Требования к средствам электронной цифровой подписи пользователей УЦ 34
7.4. Сроки действия закрытых ключей и сертификатов открытых ключей владельцев сертификатов открытых ключей 35
7.5. Служебные ключи и служебный сертификат открытого ключа 35
7.6. Рабочие ключи и рабочий сертификат открытого ключа 36
7.7. Меры защиты закрытых ключей (служебных и рабочих) 36
7.8. Копия сертификата открытого ключа электронной форме 36
7.9. Копия сертификата открытого ключа на бумажном носителе 37
7.10. Архивное хранение документированной информации 37
7.10.1. Состав архивируемых документов 37
7.10.2. Источник комплектования архивного фонда 37
7.10.3. Архивохранилище 37
7.10.4. Срок архивного хранения 37
7.10.5. Уничтожение архивных документов 38
7.11. Смена ключей уполномоченного лица Удостоверяющего Центра 38
7.11.1. Плановая смена ключей уполномоченного лица Удостоверяющего Центра 38
7.11.2. Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра 38
8. Структуры сертификатов и списков отозванных сертификатов 39
8.1. Структура сертификата открытого ключа, изготавливаемого Удостоверяющим Центром в электронной форме 39
8.1.1. Базовые поля сертификата открытого ключа 39
8.1.2. Дополнения сертификата 39
8.1.3. Объектные идентификаторы алгоритма 39
8.1.4. Формы имени 40
8.1.5. Ограничения на имена 40
8.2. Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме 41
8.2.1. Дополнения СОС 41
9. Программные и технические средства обеспечения деятельности Удостоверяющего Центра 42
9.1. Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра 42
9.2. Технические средства обеспечения работы ПК УЦ 43
9.3. Программные и программно-аппаратные средства защиты информации 43
9.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций Удостоверяющего Центра 44
9.5. Перечень данных программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра, подлежащих резервному копированию. 44
10. Обеспечение безопасности 46
10.1. Инженерно-технические меры защиты информации 46
10.1.1. Размещение технических средств Удостоверяющего Центра 46
10.1.2. Физический доступ в помещения 46
10.1.3. Электроснабжение и кондиционирование воздуха 46

10.1.4. Подверженность воздействию влаги ... 47
10.1.5. Предупреждение и защита от возгорания ... 47
10.1.6. Хранение документированной информации ... 47
10.1.7. Уничтожение документированной информации ... 47
10.2. Программно-аппаратные меры защиты информации ... 47
10.2.1. Организация доступа к техническим средствам Удостоверяющего Центра ... 47
10.2.2. Организация доступа к программным средствам Удостоверяющего Центра ... 47
10.2.3. Контроль целостности программного обеспечения ... 50
10.2.4. Контроль целостности технических средств ... 50
10.2.5. Защита внешних сетевых соединений ... 50
10.3. Организационные меры защиты информации ... 51
10.3.1. Предъявляемые требования к персоналу Удостоверяющего Центра ... 51
10.3.2. Профессиональная переподготовка и повышение квалификации персонала ... 51
10.3.3. Организация сменной работы ... 52
10.3.4. Организация доступа персонала к документам и документации ... 52
10.3.5. Охрана здания и помещений ... 52
10.4. Юридические меры защиты информации ... 52
11. Взаимодейсвтие Удостоверяющего центра с Уполномоченным федеральным органом исполнительной власти в области применения ЭЦП ... 53

Приложения

Приложение 1. Сокращения ... 54
Приложение 2. Термины и определения ... 55
Приложение 3. Структуры записей аудита ... 57

1. Введение

1.1. Обзорная информация

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего Центра (УЦ) _____ (полное наименование юридического лица) (далее по тексту – Владелец УЦ), включая обязанности пользователей (владельцев открытых ключей подписи) и членов группы администрирования УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ.

1.2. Идентификация Регламента

Наименование документа: «Регламент работы Удостоверяющего Центра».

Версия: 1.0.

Дата: ___.___.200_

Объектный идентификатор: _____.

1.3. Публикация Регламента

Настоящий Регламент распространяется:

1. в электронной форме
   a. из репозитария Владельца УЦ по адресу _____ (URL с указанием протокола);
   b. через E-mail от отправителя _____ (адрес электронной почты отправителя)
2. в бумажной форме
   a. через _____ (почтовый адрес Владельца УЦ)

Копии Регламента, предназначенные для распространения в электронной форме из репозитария Владельца УЦ, распространяются в виде двух файлов, один из которых содержит электронный образ Регламента в формате RTF, а другой - электронную цифровую подпись руководителя Удостоверяющего Центра файла электронного образа Регламента, с использованием протокола HTTP(S) с использованием протокола обеспечения безопасности информации (SSL/TLS). Файл, содержащий электронную цифровую подпись руководителя Удостоверяющего Центра, имеет формат подписанных данных PKCS#7 Signed в кодировке Base64.

Копии Регламента, предназначенные для распространения в электронной форме через E-mail, распространяются в виде файла, содержащего электронный образ Регламента в формате RTF, защищенного электронной цифровой подписью руководителя Удостоверяющего Центра с использованием S/MIME.

1.4. Область применения Регламента

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

1.5. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента – 6 лет.

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

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

Копии уведомления, предназначенные для распространения в электронной форме из репозитария Владельца УЦ, распространяются с использованием протокола HTTP(S) с использованием протокола обеспечения безопасности информации (SSL/TLS).

Копии уведомления, предназначенные для распространения в электронной форме через E-mail, защищены электронной цифровой подписью с использованием S/MIME.

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. Назначение Удостоверяющего Центра

Удостоверяющий Центр предназначен для обеспечения участников корпоративных информационных систем средствами и спецификациями для использования сертификатов открытых ключей в целях обеспечения:

- применения электронной цифровой подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- аутентификации участников информационных систем в процессе взаимодействия;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

2.2. Услуги, предоставляемые Удостоверяющим Центром

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

1. внесение в реестр Удостоверяющего Центра регистрационной информации о пользователях УЦ;
2. изготовление сертификатов открытых ключей пользователей УЦ в электронной форме;
3. изготовление копии сертификатов открытых ключей пользователей УЦ на бумажном носителе;
4. формирование закрытых и открытых ключей по обращениям пользователей УЦ с записью их на ключевой носитель;
5. ведение реестра изготовленных сертификатов открытых ключей пользователей УЦ;
6. предоставление копий сертификатов открытых ключей в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
7. аннулирование (отзыв) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
8. приостановление и возобновление действия сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
9. предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах открытых ключей;
10. подтверждение подлинности электронных цифровых подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ;
11. подтверждение подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах открытых ключей по обращениям пользователей УЦ;
12. распространение средств электронной цифровой подписи по обращениям пользователей УЦ.

2.3. Структура Удостоверяющего Центра

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

- Административная Служба УЦ;
- Служба Регистрации УЦ;

- Служба Безопасности УЦ;
- Техническая Служба УЦ.

2.3.1. Административная служба УЦ

Административная Служба УЦ предназначена для решения задач по:

- управлению деятельностью Удостоверяющего Центра;
- координации деятельности остальных Служб УЦ;
- взаимодействию с пользователями УЦ в части разрешения вопросов, связанных с применением средств ЭЦП, ключей и сертификатов открытых ключей, изготовляемых и/или распространяемых Удостоверяющим Центром;
- взаимодействию с пользователями УЦ в части разрешения вопросов, связанных с подтверждением электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификатах открытых ключей, изготовленных Удостоверяющим Центром в электронной форме, или подтверждения собственноручной подписи уполномоченного лица Удостоверяющего Центра в копиях сертификатов открытых ключей, изготовленных Удостоверяющим Центром на бумажном носителе.

2.3.2. Служба Регистрации УЦ

Служба Регистрации УЦ предназначена для решения задач по:

- регистрации пользователей УЦ;
- ведению реестра зарегистрированных пользователей УЦ;
- предоставлению служебных ключей и сертификатов открытых служебных ключей по обращению пользователей УЦ;
- распространению средств электронной цифровой подписи и шифрования.

2.3.3. Служба Безопасности УЦ

Служба Безопасности УЦ предназначена для решения задач по:

- организации и выполнению мероприятий по защите ресурсов Удостоверяющего Центра;
- изготовлению и предоставлению ключей по обращению пользователей УЦ;
- изготовлению и предоставлению изготовленных сертификатов открытых ключей в электронной форме по обращению пользователей УЦ;
- изготовлению и предоставлению копий сертификатов открытых ключей на бумажном носителе по обращению их владельцев;
- аннулированию (отзыву) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
- приостановлению и возобновлению действия сертификатов открытых ключей по обращению владельцев сертификатов открытых ключей
- предоставлению пользователям УЦ сведений об аннулированных и приостановленных сертификатах открытых ключей;
- предоставлению копий сертификатов открытых ключей, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ
- техническому обеспечению процедуры подтверждения электронной цифровой подписи в документах, представленных в электронной форме, по обращениям пользователей УЦ;
- техническому обеспечению процедуры подтверждения подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра, в изготовленных сертификатах открытых ключей, по обращениям пользователей УЦ.

2.3.4. Техническая Служба УЦ

Техническая Служба УЦ предназначена для решения задач по:

- организации и выполнению мероприятий по эксплуатации программных и технических средств обеспечения деятельности Удостоверяющего Центра;

- организации и выполнению мероприятий по техническому сопровождению распространяемых средств электронной цифровой подписи и шифрования.

2.4. Пользователи услуг Удостоверяющего Центра

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

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

Группа 2. зарегистрированные на УЦ лица, являющиеся владельцами пароля для аутентификации по паролю;

Группа 3. зарегистрированные на УЦ лица, являющиеся владельцами служебного сертификата открытого ключа;

Группа 4. зарегистрированные на УЦ лица, являющиеся владельцами рабочих сертификатов открытых ключей.

Зарегистрированные на УЦ лица, являющиеся владельцами служебных и/или рабочих сертификатов открытых ключей, все сертификаты которых признаются УЦ не действительными или не действительны по признанию УЦ соответствующие им закрытые ключи, относятся к пользователям Группы 1.

Проходить процедуру регистрации на Удостоверяющем Центре либо быть зарегистрированным пользователем может только физическое лицо.

Владельцем сертификата может быть только физическое лицо.

Физическое лицо может представлять юридическое лицо при наличии доверенности, предоставляющей права данному физическому лицу пользоваться услугами, предоставляемыми Удостоверяющим Центром, и представлять юридическое лицо.

В случае, если физическое лицо действует от имени юридического лица на основании уставных документов, в Удостоверяющий Центр представляется нотариально заверенная копия уставных документов, подтверждающих заявленные полномочия физического лица.

В тех случаях, когда сертификаты требуются для работы каких-либо устройств или программных приложений, назначается ответственное лицо, на имя которого издается сертификат.

Пользователем сертификата может быть любое лицо, устройство или программное приложение.

2.5. Разрешение споров

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

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

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

2.6. Платность услуг

Услуга Удостоверяющего Центра по предоставлению копий сертификатов открытых ключей в электронной форме, находящихся в реестре изготовленных сертификатов, предоставляется на безвозмездной основе.

Примечание. Состав и стоимость предоставляемых дополнительных услуг определяется Владельцем УЦ.

2.7. Ответственность

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

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

2.8. Прекращение деятельности

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

В случае прекращения деятельности Удостоверяющего Центра реестр Удостоверяющего Центра, включающий реестр зарегистрированных пользователей УЦ, реестр изготовленных сертификатов открытых ключей, могут передаваться в ООО «Крипто-Про» (г. Москва) по согласованию с владельцами сертификатов.

2.9. Порядок утверждения и внесения изменений в Регламент

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

Изменения в Регламент вносятся путем составления дополнительного соглашения к Регламенту.

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

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

3. Права

3.1. Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

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

3.2. Права пользователей УЦ

3.2.1. Пользователи Группы 1

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

1. Получить список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный Удостоверяющим Центром;
2. Получить сертификат открытого ключа уполномоченного лица Удостоверяющего Центра;
3. Получить копию сертификата открытого ключа в электронной форме, находящегося в Реестре сертификатов открытых ключей Удостоверяющего Центра;
4. Применять сертификат открытого ключа уполномоченного лица Удостоверяющего Центра для проверки электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификатах открытого ключа, изготовленных Удостоверяющим Центром.

5. Применять копии сертификатов открытого ключа в электронной форме для проверки электронной цифровой подписи электронного в соответствии со сведениями, указанными в сертификате открытого ключа подписи.
6. Применять список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный Удостоверяющим Центром, для проверки статуса сертификатов открытых ключей подписи.
7. Обратиться в Удостоверяющий Центр для предоставления им закрытых и открытых ключей с записью их на ключевой носитель;
8. Обратиться в Удостоверяющий Центр для внесения в реестр Удостоверяющего Центра регистрационной информации о пользователе, с целью в дальнейшем стать владельцем сертификата открытого ключа;
9. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр запрос на регистрацию в электронной форме;
10. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных цифровых подписей в документах, представленных в электронной форме;
11. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах открытых ключей;
12. Обратиться в Удостоверяющий Центр на предмет получения (приобретения) средства электронной цифровой подписи;
13. Сформировать открытые и закрытые служебные ключи на своем рабочем месте с использованием средства ЭЦП и программных средств, предоставляемых Удостоверяющим Центром.

3.2.2. Пользователи Группы 2

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

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

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

3.2.3. Пользователи Группы 3

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

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

1. Сформировать открытые и закрытые рабочие ключи на своем рабочем месте с использованием средства ЭЦП и программных средств, предоставляемых Удостоверяющим Центром;
2. Обратиться в Удостоверяющий Центр для изготовления рабочего сертификата открытого ключа;
3. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий

Центр заявление в электронной форме на изготовление рабочего сертификата открытого ключа;

4. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить и установить на свое рабочее место изготовленный рабочий сертификат открытого ключа в электронной форме;
5. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, что бы получить и установить на свое рабочее место изготовленный рабочий сертификат открытого ключа в электронной форме;
6. Обратиться в Удостоверяющий Центр для аннулирования (отзыва) служебного сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
7. Обратиться в Удостоверяющий Центр для приостановления действия служебного сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
8. Обратиться в Удостоверяющий Центр для возобновления действия служебного сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
9. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на аннулирование (отзыв) служебного сертификата открытого ключа;
10. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на приостановление действия служебного сертификата открытого ключа.

3.2.4. Пользователи Группы 4

Зарегистрированные на УЦ лица до положительного результата аутентификации по рабочему сертификату имеют права пользователей Группы 1, а также имеют право применять рабочие закрытые ключи и рабочие сертификаты открытых ключей, владельцем которых он является, для формирования электронной цифровой подписи на электронных документах в соответствии со сведениями, указанными в сертификатах открытых ключей.

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

1. Обратиться в Удостоверяющий Центр для аннулирования (отзыва) рабочего сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
2. Обратиться в Удостоверяющий Центр для приостановления действия рабочего сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
3. Обратиться в Удостоверяющий Центр для возобновления действия рабочего сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
4. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на аннулирование (отзыв) рабочего сертификата открытого ключа;
5. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы передать по сети на Удостоверяющий Центр заявление в электронной форме на приостановление действия рабочего сертификата открытого ключа;

6. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить по сети копии сертификатов открытых ключей в электронной форме из Реестра сертификатов открытых ключей Удостоверяющего Центра;

4. Обязательства

4.1. Обязательства Удостоверяющего Центра

4.1.1. Аудит

Удостоверяющий Центр обязан организовывать проверку на предмет соответствия деятельности Удостоверяющего Центра требованиям настоящего Регламента и предоставлять необходимые материалы для проверки.

Проверка Удостоверяющего Центра должна проводиться не реже одного раза в год.

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

Официальное заключение, заверенное лицом, осуществлявшим проверку, и самим Удостоверяющим Центром, Удостоверяющий Центр обязан опубликовать не позднее трех месяцев с момента окончания проверки в репозитарии Владельца УЦ по адресу _____.

4.1.2. Ключ подписи уполномоченного лица Удостоверяющего Центра

Удостоверяющий Центр обязан использовать для изготовления закрытого ключа уполномоченного лица Удостоверяющего Центра и формирования электронной цифровой подписи только средства электронной цифровой подписи, сертифицированные по классу КС2 в соответствии с действующим законодательством Российской Федерации.

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

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

4.1.3. Синхронизация времени

Удостоверяющий Центр организует работу своих Служб по GMT (Greenwich Mean Time) с учетом часового пояса.

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

4.1.4. Регистрация пользователей УЦ

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

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

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

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

4.1.5. Изготовление закрытых и открытых ключей пользователей УЦ

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

Удостоверяющий Центр обязан обеспечить сохранение в тайне изготовленного закрытого ключа.

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

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

Удостоверяющий Центр обязан обеспечить защиту ключевого носителя от копирования.

4.1.6. Изготовление сертификатов открытых ключей

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

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

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

4.1.7. Аннулирование (отзыв) сертификатов открытых ключей

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

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

4.1.8. Приостановление действия сертификатов открытых ключей

Удостоверяющий Центр обязан приостановить действие сертификат открытого ключа по заявлению его владельца.

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

4.1.9. Возобновление действия сертификатов открытых ключей

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

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

4.1.10. Уведомления

4.1.10.1. Уведомление о факте изготовлении сертификата открытого ключа

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

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

Официальным уведомлением о факте изготовлении сертификата является отправка почтового сообщения по электронной почте с прикрепленным сертификатом открытого ключа с адреса отправителя _____.

Временем отправки почтового сообщения признается время отправки почтового сообщения с почтового сервера _____, осуществляющего отправку почтовых сообщений Удостоверяющего Центра, и включенное в заголовок почтового сообщения.

4.1.10.2. Уведомление о факте аннулирования сертификата открытого ключа

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

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

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, содержащим сведения об аннулированном (отозванном) сертификате, в репозитарии Владельца УЦ по адресу _____.

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

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

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

4.1.10.3. Уведомление о факте приостановления действия сертификата открытого ключа

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

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

Официальным уведомлением о факте приостановления действия сертификата является опубликование списка отозванных сертификатов, содержащим сведения о приостановленном сертификате, в репозитарии Владельца УЦ по адресу _____.

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

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

4.1.10.4. Уведомление о факте возобновления действия сертификата открытого ключа

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

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

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

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

4.1.11. Реестр сертификатов открытых ключей

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

Реестр сертификатов открытых ключей ведется в электронном виде.

Сертификаты открытых ключей представлены в реестре в форме электронных копий изготовленных сертификатов.

Удостоверяющий Центр обязан осуществлять выдачу копий сертификатов открытых ключей в электронной форме по обращениям пользователей УЦ.

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

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

4.1.12. Прочие обязательства

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

Удостоверяющий Центр обязан обеспечить передачу пароля от рабочего места пользователя УЦ, проходящего процедуру регистрации в распределенном режиме, по защищенным каналам связи, реализуемого шифровальными (криптографическими) средствами, сертифицированными не ниже уровня «КС1».

4.2. Обязательства пользователей УЦ

4.2.1. Обязанности лиц, проходящих процедуру регистрации

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

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

4.2.2. Обязанности владельцев закрытых ключей

Владелец закрытого ключа обязан:

- хранить в тайне закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
- не использовать для электронной цифровой подписи закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;
- использовать закрытый ключ только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту.

4.2.3. Обязанности владельца сертификата открытого ключа

Владелец сертификата открытого ключа, изданного Удостоверяющим Центром, обязан:

- использовать сертификат открытого ключа только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;
- немедленно обратиться в Удостоверяющий Центр с заявлением на аннулирование (отзыв) сертификата открытого ключа в случае, если ему известно, что эти ключи используются или использовались ранее другими лицами.

4.2.4. Обязанности пользователей сертификатов открытых ключей

Перед тем как использовать сертификат открытого ключа, изготовленный Удостоверяющим Центром, пользователь сертификата (пользователь, не являющийся его владельцем) должен удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту, соответствует предполагаемому использованию.

5. Политика конфиденциальности

5.1. Типы конфиденциальной информации

Закрытый ключ владельца сертификата открытого ключа является конфиденциальной информацией данного пользователя УЦ. Удостоверяющий Центр не депонирует и не архивирует закрытые ключи.

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

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

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

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

5.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

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

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

Также не считается конфиденциальной информация о настоящем Регламенте.

5.3. Исключительные полномочия официальных лиц

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

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

6. Процедуры и механизмы

6.1. Процедура регистрации пользователей УЦ

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

Процедура регистрации пользователей УЦ применяется в отношении физических лиц, обращающихся к услугам Удостоверяющего Центра в части изготовления сертификатов открытых ключей пользователей УЦ и/или формирования закрытых и открытых ключей пользователей УЦ с записью их на ключевой носитель.

6.1.1. Заявление на регистрацию

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

Заявление должно содержать следующие обязательные реквизиты:

- Для физического лица:
  - Идентификационные данные, включающие:
    - Фамилию, имя и отчество;
    - Адрес электронной почты.
  - Паспортные данные (или другого документа, удостоверяющего личность)
    - Вид документа;
    - Серия паспорта;
    - Номер паспорта;
    - Кем выдан;
    - Когда выдан.
  - Контактные телефоны
  - Данные для удаленной идентификации (ключевая фраза) до 64 символов
- Для физического лица, представляющего юридическое лицо
  - Идентификационные данные, включающие:
    - Фамилию, имя и отчество;
    - Адрес электронной почты;
    - Наименование организации;
    - Субъект Федерации, в котором зарегистрирована организация;
    - Должность.
  - Данные доверенности (или других документов, подтверждающих правомочность действий от имени юридического лица)
  - Данные для удаленной идентификации информация (ключевая фраза) до 64 символов

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.

6.1.2. Идентификация пользователя УЦ

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

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

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

6.1.3. Регистрация пользователя УЦ в централизованном режиме

Регистрация пользователя УЦ в централизованном режиме осуществляется сотрудником Службы Регистрации УЦ на основе заявления на регистрацию при личном прибытии лица, проходящего процедуру регистрации, в офис Удостоверяющего Центра, расположенный по адресу _____.

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

После положительной идентификации лица, проходящего процедуру регистрации, сотрудник Службы Регистрации УЦ подготавливает бланк заявления на регистрацию и передает его заявителю.

Заявитель заверяет заявление на регистрацию собственноручной подписью и передает заявление вместе с необходимыми приложениями сотруднику Службы Регистрации УЦ.

Заявление на регистрацию рассматривается Службой Регистрации 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, сотрудник Службы Регистрации УЦ выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего Центра и изготавливает служебные ключи и служебный сертификат открытого ключа (в соответствии с пунктом 7.5 настоящего Регламента).

Заявление на изготовление служебных ключей и сертификата открытого ключа подается заявителем в соответствии с дополнительным соглашением или устно.

По окончании процедуры регистрации, зарегистрированному пользователю УЦ выдаются:

- ключи, записанные на ключевой носитель;
- сертификат открытого ключа в электронной форме, соответствующий закрытому ключу;
- копия сертификата открытого ключа на бумажном носителе по форме, определенной настоящим Регламентом;
- копии сертификатов открытого ключа в электронной форме уполномоченного лица Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии;
- списки отозванных сертификатов в электронной форме Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии.

Указанные выше данные, передаваемые зарегистрированному пользователю в электронной форме, записываются в виде файлов на дискету 3,5”.

По необходимости (в случае его отсутствия у пользователя), регистрируемый пользователь УЦ должен приобрести (получить) средство электронной подписи и шифрования, распространяемое Удостоверяющим Центром.

6.1.4. Регистрация пользователя УЦ в распределенном режиме

Регистрация пользователя УЦ в распределенном режиме осуществляется сотрудником Службы Регистрации УЦ на основании нотариально заверенного заявления на регистрацию лица, проходящего процедуру регистрации, поступившего в офис Удостоверяющего Центра, расположенный по адресу _____, и на основании запроса на регистрацию в электронной форме, поступившего в Удостоверяющий Центр.

Идентификация лица, проходящего процедуру регистрации, выполняется нотариусом в процессе совершения нотариальных действий по заверению заявления на регистрацию.

Сотрудник Службы Регистрации УЦ выполняет процедуру проверки соответствия идентификационных данных, поступивших в запросе на регистрацию в электронной форме и в заявлении на регистрацию в бумажной форме.

Регистрация пользователя УЦ в распределенном режиме осуществляется с использованием программных средств, предоставляемых Удостоверяющим Центром.

Перед началом процедуры регистрации в распределенном режиме, пользователь должен получить средство электронной подписи и шифрования, распространяемое Удостоверяющим Центром.

В комплект средства электронной подписи и шифрования должны входить сертификаты в электронной форме Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии, а также списки отозванных сертификатов в электронной форме Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии.

Лицо, проходящее процедуру регистрации в распределенном режиме, должно с использованием программного обеспечения регистрации пользователя УЦ, предоставляемого Удостоверяющим Центром, сформировать и отправить в Удостоверяющий Центр запрос на регистрацию в электронном виде.

В процессе формирования и отправки запроса на регистрацию в электронном виде, лицо, проходящее процедуру регистрации, получает пароль, сформированный Удостоверяющим Центром, для аутентификации пользователя УЦ по паролю.

После отправки запроса на регистрацию в электронном виде, лицо, проходящее процедуру регистрации, должно выслать почтовым сообщением с уведомлением о вручении в Службу Регистрации УЦ нотариально заверенное заявление на регистрацию (в соответствии с пунктом 6.1.1 настоящего Регламента).

Заявление на регистрацию рассматривается Службой Регистрации УЦ в течение 2 рабочих дней с его момента поступления в Службу.

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

Официальным уведомлением пользователя УЦ об отказе в регистрации является отправка почтового сообщения через E-mail от отправителя _____ (адрес электронной почты отправителя).

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

Официальным уведомлением пользователя УЦ о регистрации является отправка почтового сообщения через E-mail от отправителя _____ (адрес электронной почты отправителя).

Зарегистрированный пользователь УЦ должен с использованием программного обеспечения регистрации пользователя УЦ, предоставляемого Удостоверяющим Центром, выполнить процедуру генерации служебных ключей, сформировать и отправить в Удостоверяющий Центр запрос на служебный сертификат открытого ключа в электронном виде и заявление на служебный сертификат открытого ключа в бумажном виде.

Заявление на служебный сертификат открытого ключа в бумажном виде рассматривается Службой Регистрации УЦ в течение 2 рабочих дней с его момента поступления в Службу.

Официальным уведомлением пользователя УЦ о выпуске служебного сертификата открытого ключа является отправка почтового сообщения через E-mail от отправителя _____ (адрес электронной почты отправителя).

Зарегистрированный пользователь УЦ должен с использованием программного обеспечения регистрации пользователя УЦ, предоставляемого Удостоверяющим Центром, выполнить процедуру установки выпущенного сертификата открытого ключа на рабочее место.

После выполнения процедуры установки выпущенного сертификата открытого ключа на рабочее место аутентификация зарегистрированного пользователя УЦ по паролю становится недоступной.

После выполнения процедуры установки служебного сертификата открытого ключа на рабочее место, пользователь УЦ должен с использованием программного обеспечения зарегистрированного пользователя УЦ, предоставляемого Удостоверяющим Центром, выполнить процедуру генерации рабочих ключей, сформировать и отправить в Удостоверяющий Центр заявление на рабочий сертификат открытого ключа в электронном виде.

Заявление на рабочий сертификат открытого ключа в электронном виде рассматривается Службой Безопасности УЦ в течение 3 рабочих дней с момента поступления в Службу Безопасности УЦ копий служебного сертификата открытого ключа на бумажном носителе.

Официальным уведомлением пользователя УЦ о выпуске рабочего сертификата открытого ключа является отправка почтового сообщения через E-mail от отправителя _____ (адрес электронной почты отправителя).

Отсутствие в течение 3 рабочих дней официального уведомления пользователя УЦ о выпуске рабочего сертификата открытого ключа является официальным отказом в изготовлении рабочего сертификата открытого ключа.

Зарегистрированный пользователь УЦ должен с использованием программного обеспечения зарегистрированного пользователя УЦ, предоставляемого Удостоверяющим Центром, выполнить процедуру установки выпущенного рабочего сертификата открытого ключа на рабочее место.

6.2. Идентификация зарегистрированного пользователя

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

6.3. Аутентификация зарегистрированного пользователя

6.3.1. Очная аутентификация зарегистрированного пользователя

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

6.3.2. Удаленная аутентификация зарегистрированного пользователя

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

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

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

6.3.3. Аутентификация зарегистрированного пользователя по сертификату открытого ключа

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

6.3.4. Аутентификация зарегистрированного пользователя по паролю

Аутентификация зарегистрированного пользователя УЦ по паролю выполняется путем сопоставления предъявленного зарегистрированным пользователем УЦ пароля с учетной информацией, хранимой в Реестре зарегистрированных пользователей Удостоверяющего Центра.

Действие пароля начинается с момента его предоставления пользователю УЦ.

Срок действия пароля составляет 30 календарных суток или ограничивается по времени моментом установки выпущенного Удостоверяющим Центром сертификата открытого ключа на рабочее место зарегистрированного пользователя УЦ (что наступит раньше).

6.4. Изготовление ключей

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

6.4.1. Заявление на изготовление ключей

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

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

Заявление на изготовление ключей рассматривается Службой Безопасности УЦ в течение 30 минут с момента поступления.

6.4.2. Изготовление и выдача ключей владельцу

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

Изготовление ключей осуществляется в присутствии заявителя.

Изготовленные ключи записываются на ключевой носитель, предоставляемый заявителем.

Предоставляемый заявителем ключевой носитель должен удовлетворять следующим требованиям:

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

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

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

6.5. Изготовление сертификата открытого ключа и предоставление его владельцу

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

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

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

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

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

После изготовления сертификата открытого ключа его владельцу направляется официальное уведомление (см. раздел 4.1.10 настоящего Регламента).

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

Копия сертификата открытого ключа на бумажном носителе предоставляется его владельцу при личном обращении в Службу Безопасности УЦ.

6.5.1. Заявление на изготовление сертификата открытого ключа в электронной форме

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

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

6.5.2. Заявление на изготовление сертификата открытого ключа в бумажной форме

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

Заявление включает в себя следующие обязательные реквизиты:

- Фамилию, имя, отчество заявителя;
- Дату и подпись заявителя;
- Текст запроса на сертификат в формате PKCS#10 в кодировке Base64.

Обязательным приложением к заявлению на изготовление сертификата открытого ключа в бумажной форме является файл, содержащий запрос на сертификат в формате PKCS#10 в кодировке Base64, размещенный на магнитном носителе (дискета 3’5”).

6.5.3. Идентификация владельца сертификата открытого ключа

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

6.6. Аннулирование (отзыв) сертификата открытого ключа

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

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

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

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

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

После аннулирования (отзыва) сертификата открытого ключа его владельцу направляется официальное уведомление (см. раздел 4.1.10 настоящего Регламента).

6.6.1. Заявление на отзыв сертификата открытого ключа в электронной форме

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

Запрос на отзыв сертификата представляет собой строку формата «SN=CertificateSerialNumber,RR=Reason,RC=SomeComment», где:

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

6.6.2. Заявление на отзыв сертификата открытого ключа в бумажной форме

Заявление на отзыв сертификата открытого ключа в бумажной 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. Приостановление действия сертификата открытого ключа

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

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

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

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

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

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

После приостановления действия сертификата открытого ключа его владельцу направляется официальное уведомление (см. раздел 4.1.10 настоящего Регламента).

6.7.1. Заявление на приостановление действия сертификата открытого ключа в электронной форме

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

Запрос на приостановление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber,RR=Reason,RC=SomeComment,HD=x-x-x-x-x-x», где:

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

6.7.2. Заявление на приостановление действия сертификата открытого ключа в бумажной форме

Заявление на приостановление действия сертификата открытого ключа в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

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

6.7.3. Заявление на приостановление действия сертификата открытого ключа в устной форме

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

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

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

6.8. Возобновление действия сертификата открытого ключа

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

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

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

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

Срок рассмотрения заявления на возобновление действия сертификата открытого ключа составляет 3 рабочих дня с момента его поступления в Службу Безопасности УЦ.

После возобновления действия сертификата открытого ключа его владельцу направляется официальное уведомление (см. раздел 4.1.10 настоящего Регламента).

6.8.1. Заявление на возобновление действия сертификата открытого ключа в электронной форме

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

Запрос на возобновление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber,RR=Reason,RC=SomeComment», где:

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

6.8.2. Заявление на возобновление действия сертификата открытого ключа в бумажной форме

Заявление на возобновление действия сертификата открытого ключа в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление включает в себя следующие обязательные реквизиты:

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

6.9. Срок хранения сертификата открытого ключа

Хранение сертификата открытого ключа пользователей УЦ в Реестре сертификатов открытых ключей Удостоверяющим Центром, осуществляется в течение установленного срока действия сертификата открытого ключа.

Срок архивного хранения сертификата открытого ключа устанавливается в соответствии со сроком, определенным разделом 7.10 настоящего Регламента.

6.10. Процедура подтверждения электронной цифровой подписи с использованием сертификата открытого ключа

Подтверждение электронной цифровой подписи в электронном документе осуществляется Удостоверяющим Центром по обращению граждан (далее по тексту раздела – заявитель), на основании заявления на подтверждение электронной цифровой подписи в электронном документе в простой письменной форме.

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

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

Бремя доказывания достоверности даты и времени формирования электронной цифровой подписи в электронном документе возлагается на заявителя.

Обязательным приложением к заявлению на подтверждение электронной цифровой подписи в электронном документе является магнитный носитель (дискета 3’5”), содержащий следующие файлы:

- Файл, содержащий электронный документ, к которому применена электронная цифровая подпись;
- Файл, содержащий электронную цифровую подпись формата PKCS#7 электронного документа, к которому применена электронная цифровая подпись;
- Файл, содержащий сертификат открытого ключа уполномоченного лица Удостоверяющего Центра, являющегося издателем сертификата открытого ключа электронной цифровой подписи электронного документа;
- Файл, содержащий список отозванных сертификатов Удостоверяющего Центра, являющегося издателем сертификата открытого ключа электронной цифровой подписи электронного документа, и использовавшийся для проверки электронной цифровой подписи электронного документа заявителем.

Срок рассмотрения заявления на подтверждение электронной цифровой подписи в электронном документе составляет 5 рабочих дней с момента его поступления в Административную Службу УЦ.

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

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

Ответ содержит:

- результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в

подписанном данной электронной цифровой подписью электронном документе;

- детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

6.11. Процедура подтверждения электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификате открытого ключа

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

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

Обязательным приложением к заявлению на подтверждение электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификате открытого ключа является магнитный носитель (дискета 3’5”), содержащий следующие файлы:

- Файл, содержащий сертификат открытого ключа зарегистрированного пользователя УЦ, подвергающийся процедуре проверки;
- Файл, содержащий сертификат открытого ключа уполномоченного лица Удостоверяющего Центра, являющегося издателем сертификата открытого ключа пользователя УЦ, подвергающегося процедуре проверки;
- Файл, содержащий список отозванных сертификатов Удостоверяющего Центра, являющегося издателем сертификата открытого ключа, и использовавшийся для проверки электронной цифровой подписи уполномоченного лица Удостоверяющего Центра заявителем.

Срок рассмотрения заявления на подтверждение электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификате открытого ключа составляет 5 рабочих дней с момента его поступления в Административную Службу УЦ.

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

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

Ответ содержит:

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

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с федеральным законом.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

6.12. Механизм доказательства обладания закрытым ключом, соответствующим открытому ключу

Заявления на изготовление сертификатов открытых ключей, поступающие в Удостоверяющий Центр от владельцев закрытых и открытых ключей, должны содержать собственноручную подпись заявителя и, в качестве реквизита, запрос на сертификат, подготовленный в соответствии с форматом криптографических сообщений PKCS#10 в формате Base64 с заголовком или без оного.

Подтверждение цифровой подписи запроса на сертификат из заявления на изготовление сертификатов открытых ключей и наличие собственноручной подписи заявителя подтверждает, что заявитель является владельцем закрытого ключа, соответствующего открытому ключу из заявления на изготовление сертификатов открытых ключей.

7. Дополнительные положения

7.1. Идентифицирующие данные уполномоченного лица Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра идентифицируется по следующим данным:

- Фамилия, имя отчество: _____
- Организация: _____
- Подразделение: _____
- Адрес электронной почты: _____
- Субъект Федерации: _____

7.2. Сроки действия ключей уполномоченного лица Удостоверяющего Центра

Срок действия закрытого ключа уполномоченного лица Удостоверяющего центра составляет 3 года.

В течение 1 года 3 месяцев с момента начала срока действия закрытого ключа уполномоченного лица Удостоверяющего центра закрытый ключ уполномоченного лица удостоверяющего центра используется для изготовления сертификатов пользователей и формирования списков отозванных сертификатов.

По истечении 1 года 3 месяцев и до окончания срока действия закрытого ключа уполномоченного лица Удостоверяющего центра данный закрытый ключ используется исключительно для формирования списков отозванных сертификатов Удостоверяющего центра.

Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего Центра исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа.

Срок действия сертификата открытого ключа, соответствующего закрытому ключу уполномоченного лица Удостоверяющего Центра, составляет 30 лет.

7.3. Требования к средствам электронной цифровой подписи пользователей УЦ

Средство электронной цифровой подписи должно обеспечивать выполнение следующих процедур:

- Генерацию закрытых и открытых ключей;
- Формирование электронной цифровой подписи;
- Проверку электронной цифровой подписи.

Средство электронной цифровой подписи должно обеспечивать выполнение мер защиты закрытых ключей (см. раздел 7.7).

В качестве средства электронной цифровой подписи пользователи должны использовать сертифицированные в соответствии с правилами сертификации средства криптографической защиты информации по уровню защиты не ниже «КС1».

Средства криптографической защиты информации должны быть разработаны в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

Идентификаторы алгоритмов должны быть зарегистрированы в настоящем Регламенте в разделе 8.1.3.

Средства криптографической защиты информации должны удовлетворять по форматам и параметрам криптографических алгоритмов требованиям, изложенным в

документе "Рекомендации к средствам криптографической защиты информации на взаимодействие удостоверяющих центров, реестров сертификатов, сертификаты ключей формата X.509 и электронные документы формата CMS", разработанного ООО "Крипто-Про". Авторские права подтверждены заявкой № 2001129024 ("Цифровой сертификат открытого ключа"), зарегистрированной в Российском агентстве по патентам и товарным знакам.

7.4. Сроки действия закрытых ключей и сертификатов открытых ключей владельцев сертификатов открытых ключей

Максимальный срок действия закрытого ключа пользователя УЦ, соответствующего сертификату открытого ключа, владельцем которого он является, составляет 1 год 3 месяца.

Начало периода действия закрытого ключа пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа пользователя УЦ.

Срок действия открытого ключа устанавливается равным сроку действия сертификата открытого ключа.

Максимальный срок, который может быть установлен в качестве срока действия сертификатов открытых ключей пользователей УЦ, составляет 30 лет.

Срок действия сертификата открытого ключа устанавливается Удостоверяющим Центром в момент его изготовления.

Срок действия сертификата открытого ключа пользователя УЦ определяется путем выбора минимального из установленных сроков областей использования сертификатов, приведенных в Таблица 1, из числа областей использования, указанных в соответствующем заявлении на изготовление сертификата открытого ключа.

Таблица 1. Пример таблицы сроков областей использования сертификатов

№ п/п	Наименование области использования	Объектный идентификатор	Срок
1.	Центр Регистрации	1.2.643.2.2.34.7	1 год 3 месяца
2.	Администратор Центра Регистрации	1.2.643.2.2.34.4	1 год 3 месяца
3.	Оператор Центра Регистрации	1.2.643.2.2.34.5	1 год 3 месяца
4.	Пользователь Центра Регистрации	1.2.643.2.2.34.6	1 год 3 месяца
5.	Временный доступ к Центру Регистрации	1.2.643.2.2.34.2	1 неделя
6.	Защищенная электронная почта	1.3.6.1.5.5.7.3.4	5 лет
7.	Проверка подлинности клиента	1.3.6.1.5.5.7.3.2	1 год 3 месяца
8.	Проверка подлинности сервера	1.3.6.1.5.5.7.3.1	1 год 3 месяца

7.5. Служебные ключи и служебный сертификат открытого ключа

Служебные ключи и служебный сертификат открытого ключа предназначены только для:

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

Служебный сертификат открытого ключа содержит следующие области использования:

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

Срок действия закрытого служебного ключа устанавливается равным сроку действия соответствующего служебного открытого ключа.

Срок действия служебного открытого ключа устанавливается равным сроку действия служебного сертификата открытого ключа.

Срок действия служебного открытого ключа устанавливается равным сроку, соответствующему области использования «Временный доступ к Центру Регистрации» из Таблица 1.

7.6. Рабочие ключи и рабочий сертификат открытого ключа

Рабочие ключи и рабочий сертификат открытого ключа предназначены для:

- обеспечения аутентификации и авторизации зарегистрированного пользователя УЦ при использовании программного обеспечения зарегистрированного пользователя УЦ, предоставляемого Удостоверяющим Центром;
- формирования электронной цифровой подписи в заявлении на рабочий сертификат открытого ключа в электронном виде;
- использования в соответствии со сведениями, указанными в сертификате в областях использования.

7.7. Меры защиты закрытых ключей (служебных и рабочих)

Закрытые ключи пользователей УЦ должны записываться при их генерации на отчуждаемые (относительно рабочего места) магнитные носители ключевой информации.

В качестве таких носителей ключевой информации допускается использовать только носители, указанные в формуляре средства электронной цифровой подписи, использовавшегося при их генерации.

Закрытые ключи на магнитном носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, учитывая следующие требования:

- Длин пароля (ПИН-кода) не должна быть меньше 6 символов;
- Пароль (ПИН-код) должен содержать символы цифр и букв латинского алфавита.

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

Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца закрытых ключей.

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

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

7.8. Копия сертификата открытого ключа электронной форме

Копия сертификата открытого ключа пользователя УЦ в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту Международного союза телекоммуникаций ITU-T X.509 версии 3 и

рекомендаций IETF (Internet Engineering Task Force) RFC 2459, и представленный в кодировке Base64.

7.9. Копия сертификата открытого ключа на бумажном носителе

Копия сертификата открытого ключа пользователя УЦ на бумажном носителе, представляет собой документ, содержащий следующие обязательные реквизиты:

- Серийный номер сертификата открытого ключа;
- Идентификационные данные владельца сертификата;
- Идентификационные данные издателя сертификата (идентификационные данные из сертификата открытого ключа уполномоченного лица Удостоверяющего Центра);
- Сведения о средстве ЭЦП уполномоченного лица Удостоверяющего Центра;
- Сведения об открытом ключе владельца сертификата и алгоритме его формирования;
- Сведения об областях использования закрытого ключа и сертификата;
- Собственноручную подпись уполномоченного лица Удостоверяющего Центра;
- Печать УЦ.

Копия сертификата открытого ключа печатается на листах белой бумаги формата А4, не содержащих средств защиты от копирования и подделки.

7.10. Архивное хранение документированной информации

7.10.1. Состав архивируемых документов

Архивированию подлежат следующая документированная информация:

- Реестр сертификатов открытых ключей пользователей УЦ;
- сертификаты открытых ключей уполномоченного лица Удостоверяющего Центра;
- журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего Центра;
- Реестр зарегистрированных пользователей Удостоверяющего Центра;
- заявления на изготовление ключей пользователей УЦ;
- заявления на изготовление сертификатов открытых ключей пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов открытых ключей;
- заявления на приостановление действия сертификатов открытых ключей;
- заявления на возобновление действия сертификатов открытых ключей:
- служебные документы Удостоверяющего Центра.

7.10.2. Источник комплектования архивного фонда

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

7.10.3. Архивохранилище

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

7.10.4. Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов устанавливается 11 лет.

7.10.5. Уничтожение архивных документов

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

7.11. Смена ключей уполномоченного лица Удостоверяющего Центра

7.11.1. Плановая смена ключей уполномоченного лица Удостоверяющего Центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица Удостоверяющего Центра выполняется не ранее, чем через 1 год, и не позднее, чем через 1 год и 3 месяца после начала действия закрытого ключа уполномоченного лица Удостоверяющего Центра.

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

- Уполномоченное лицо Удостоверяющего Центра формирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового открытого ключа и подписывает его электронной цифровой подписью с использованием нового закрытого ключа.

Старый закрытый ключ уполномоченного лица Удостоверяющего Центра используется в течении 1 года с момента изготовления сертификата нового открытого ключа уполномоченного лица Удостоверяющего Центра для формирования списков отозванных сертификатов в электронной форме, изданных Удостоверяющим Центром в период действия старого закрытого ключа уполномоченного лица Удостоверяющего Центра.

7.11.2. Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра

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

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

После выполнения процедуры внеплановой смены ключей уполномоченного лица Удостоверяющего Центра, сертификат открытого ключа уполномоченного лица Удостоверяющего Центра аннулируется (отзывается) путем занесения в список отозванных сертификатов.

8. Структуры сертификатов и списков отозванных сертификатов

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

Удостоверяющий Центр издает сертификаты открытых ключей пользователей УЦ и уполномоченного лица Удостоверяющего Центра в электронной форме (далее по тексту раздела – сертификаты открытых ключей) формата X.509 версии 3.

8.1.1. Базовые поля сертификата открытого ключа

Сертификаты открытых ключей содержат следующие базовые поля X.509:

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

8.1.2. Дополнения сертификата

Сертификаты открытых ключей содержат следующие дополнения:

authorityKeyIdentifier	идентификатор ключа уполномоченного лица Удостоверяющего Центра
subjectKeyIdentifier	идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение
cRLDistributionPoint	точка распространения списка аннулированных (отозванных) сертификатов открытых ключей, изданных Удостоверяющим Центром
KeyUsage	Назначение ключа

8.1.3. Объектные идентификаторы алгоритма

Удостоверяющий Центр использует следующие идентификаторы алгоритмов средства электронной цифровой подписи, имеющего наименование «СКЗИ КриптоПро CSP»:

ГОСТ Р 34.10-94	1.2.643.2.2.20
Диффи-Хеллмана	1.2.643.2.2.99

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

8.1.4. Формы имени

В сертификате открытого ключа поля идентификационных данных уполномоченного лица Удостоверяющего Центра и владельца сертификата содержат атрибуты имени формата X.500.

8.1.5. Ограничения на имена

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего Центра являются:

Common Name	Фамилия, имя, отчество
Organization	Наименование организации, являющейся владельцем Удостоверяющего Центра
Organization Unit	Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего Центра
Email	Адрес электронной почты
Country	RU
State	Субъект Федерации, где зарегистрирована организация, являющейся владельцем Удостоверяющего Центра

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

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

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

Common Name	Фамилия, имя, отчество
Organization	Наименование организации, которую представляет владелец сертификата
Organization Unit	Наименование подразделения организации, сотрудником которого является владелец сертификата
Email	Адрес электронной почты
Country	RU
State	Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата

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

Удостоверяющий Центр издает списки отозванных сертификатов открытых ключей пользователей УЦ и уполномоченного лица Удостоверяющего Центра в электронной форме (далее по тексту раздела – СОС) формата X.509 версии 2.

8.2.1. Дополнения СОС

Удостоверяющий Центр использует следующие дополнения:

Authority Key Identifier	идентификатор ключа уполномоченного лица Удостоверяющего Центра
Reason Code	Код причины отзыва сертификата открытого ключа
szOID_CERTSRV_CA_VERSION	Объектный идентификатор MS Certificate Server, определяющий версию службы сертификации MS CA

9. Программные и технические средства обеспечения деятельности Удостоверяющего Центра

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

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

9.1. Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра

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

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

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

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

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

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

1. Ведения Реестра зарегистрированных пользователей Удостоверяющего Центра;
2. Ведения Реестра сертификатов открытых ключей Удостоверяющего Центра;
3. Ведения Реестра заявлений на изготовление сертификатов открытых ключей пользователей УЦ в электронной форме;
4. Ведения Реестра заявлений на аннулирование (отзыв) сертификатов открытых ключей пользователей УЦ в электронной форме;

5. Ведения Реестра заявлений на приостановление действия сертификатов открытых ключей пользователей УЦ в электронной форме;
6. Ведения Реестра запросов на регистрацию пользователей УЦ в электронной форме;
7. Ведения Реестра заявлений на возобновление действия сертификатов открытых ключей пользователей УЦ в электронной форме;
8. Предоставления программных средств для:
    a. Пользователей УЦ Группы 1 для обеспечения реализации их права передать по сети на Удостоверяющий Центр запрос на регистрацию в электронной форме;
    b. Зарегистрированных пользователей УЦ Группы 2 и 3 для обеспечения реализации их прав в части пользования предоставляемыми программными средствами;

Ответственность за эксплуатацию Центра Регистрации возлагается на Службу Регистрации УЦ.

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

АРМ разбора конфликтных ситуаций является приложением ПК УЦ и предназначен для обеспечения своих функциональных обязанностей сотрудникам Административной Службы УЦ в части взаимодействия с пользователями УЦ при разрешении вопросов, связанных с подтверждением электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификатах открытых ключей, изготовленных Удостоверяющим Центром в электронной форме.

9.2. Технические средства обеспечения работы ПК УЦ

Технические средства обеспечения работы ПК УЦ включают в себя:

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

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

9.3. Программные и программно-аппаратные средства защиты информации

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

- Средства криптографической защиты информации;
- Межсетевой экран для обеспечения защиты информации при сетевом взаимодействии с Центром Регистрации;
- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Устройства обеспечения бесперебойного питания серверов Центра Сертификации и Центра Регистрации;

- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений Удостоверяющего Центра;
- Устройства обеспечения противопожарной безопасности помещений Удостоверяющего Центра.

Средства криптографической защиты информации, эксплуатируемые на всех компонентах ПК УЦ, должны быть сертифицированы по классу «КС2» в соответствии с действующим законодательством Российской Федерации.

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

9.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций Удостоверяющего Центра

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

Структуры записей событий приведены в эксплуатационной документации программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра и общесистемного программного обеспечения.

9.5. Перечень данных программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра, подлежащих резервному копированию.

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

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

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

10. Обеспечение безопасности

10.1. Инженерно-технические меры защиты информации

10.1.1. Размещение технических средств Удостоверяющего Центра

Сервера Центра Сертификации, Центра Регистрации и телекоммуникационное оборудование должны быть размещены в выделенном помещении (далее по тексту – серверное помещение).

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

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

10.1.2. Физический доступ в помещения

Серверное помещение Удостоверяющего Центра оборудовано системой контроля доступа с идентификацией по карте.

Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

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

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

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

10.1.3. Электроснабжение и кондиционирование воздуха

Технические средства Удостоверяющего Центра подключены к общегородской сети электроснабжения.

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

Сервера Центра Сертификации и Центра Регистрации, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение 8 часов после прекращения основного электроснабжения.

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

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

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

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

10.1.4. Подверженность воздействию влаги

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

10.1.5. Предупреждение и защита от возгорания

Серверное помещение Удостоверяющего Центра оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

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

10.1.6. Хранение документированной информации

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

10.1.7. Уничтожение документированной информации

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

10.2. Программно-аппаратные меры защиты информации

10.2.1. Организация доступа к техническим средствам Удостоверяющего Центра

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

Идентификационные карты доступа в серверное помещение выдаются сотрудникам на основании приказа руководителя Удостоверяющего Центра.

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

10.2.2. Организация доступа к программным средствам Удостоверяющего Центра

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

Рабочие места сотрудников Удостоверяющего Центра, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» также оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок».

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

10.2.2.1. Общий перечень объектов доступа УЦ

К объектам доступа Удостоверяющего центра относятся:

- технические средства компонент УЦ;
- программное обеспечение компонент УЦ: ПО центра сертификации, ПО Центра регистрации, ПО АРМ администратора Центра регистрации, ПО АРМ разбора конфликтных ситуаций, ПО, продназначенное для регистрации и управления сертификатами пользователей УЦ;

- базы данных компонент УЦ: база данных ЦС, база данных ЦР;
- закрытые ключи и сертификаты открытых ключей;
- списки отозванных сертификатов УЦ.

10.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам Удостоверяющего центра

Сотрудникам Административной Службы УЦ:

- технические средства Центра сертификации и Центра регистрации УЦ;
- технические средства АРМ разбора конфликтных ситуаций;
- программное обеспечение Центра сертификации и Центра регистрации УЦ;
- база данных Центра сертификации и Центра регистрации УЦ;
- закрытые ключи и сертификаты открытых ключей, использующиеся для эксплуатации Центра сертификации и Центра регистрации;
- списки отозванных сертификатов УЦ.

Сотрудникам Службы Регистрации УЦ:

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

Сотрудникам Службы Безопасности УЦ:

- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные закрытые ключи и сертификаты открытых ключей сотрудников Службы Безопасности;
- служебные сертификаты открытых ключей пользователей УЦ;
- рабочие ключи и рабочие сертификаты открытых ключей пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам Технической службы УЦ:

- технические средства компонент УЦ;
- программное обеспечение компонент УЦ;
- базы данных Центра сертификации и Центра регистрации.

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

Пользователям УЦ Группы 1:

- программное обеспечение формирования запроса на регистрацию пользователя УЦ;

Пользователям УЦ Группы 2:

- программное обеспечение формирования служебных ключей и запроса на служебный сертификат открытого ключа аутентифицированного пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изданного служебного сертификата открытого ключа аутентифицированного пользователя УЦ;

- программное обеспечение формирования электронного бланка копии изданного служебного сертификата открытого ключа аутентифицированного пользователя УЦ в бумажной форме;
- личные служебные ключи и служебные сертификаты открытых ключей.

Пользователям УЦ Группы 3:

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

Пользователям УЦ Группы 4:

- копия сертификата открытого ключа уполномоченного лица Удостоверяющего Центра в электронной форме;
- копия списка аннулированных (отозванных) сертификатов открытых ключей в электронной форме;
- копии сертификатов открытых ключей пользователей Удостоверяющего Центра в электронной форме;
- программное обеспечение предоставления учетной информации о сертификатах открытых ключей аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение предоставления учетной информации о запросах (заявлениях) в электронной форме, поступивших на Удостоверяющий Центр от аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение формирования рабочих ключей и заявления на рабочий сертификат открытого ключа в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изданного рабочего сертификата открытого ключа аутентифицированного пользователя УЦ;

- программное обеспечение формирования электронного бланка копии служебного сертификата открытого ключа аутентифицированного пользователя УЦ в бумажной форме;
- программное обеспечение формирования заявления на аннулирование (отзыв) служебного сертификата открытого ключа в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение формирования заявления на приостановление действия служебного сертификата открытого ключа в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение формирования заявления на возобновление действия служебного сертификата открытого ключа в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение предоставления учетной информации о сертификатах открытых ключей пользователей УЦ и копий сертификатов открытых ключей пользователей УЦ в электронной форме.
- личные рабочие ключи и рабочие сертификаты открытых ключей.

10.2.3. Контроль целостности программного обеспечения

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

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

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

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

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

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

Периодичность выполнения мероприятий по контролю целостности – ежесуточно.

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

10.2.4. Контроль целостности технических средств

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

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

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

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

10.2.5. Защита внешних сетевых соединений

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

В качестве шифровальных (криптографических) средств пользователей УЦ, используемых для защиты конфиденциальной информации, используется средство электронной цифровой подписи пользователя УЦ.

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

10.2.5.1. Перечень информации, подлежащей защите

Поступающая в Удостоверяющий Центр информация:

- Заявление на регистрацию в электронной форме;
- Заявление на изготовление сертификата открытого ключа в электронной форме;
- Заявление на аннулирование (отзыв) сертификата открытого ключа в электронной форме;
- Заявление на приостановление действия сертификата открытого ключа в электронной форме;
- Заявление на возобновление действия сертификата открытого ключа в электронной форме;
- Пароль, передаваемый пользователем УЦ при аутентификации по паролю;
- Ключевая фраза пользователя УЦ.

Передаваемая из Удостоверяющего Центра информация:

- Пароль, передаваемый пользователю УЦ для аутентификации по паролю;
- Бланк копии сертификата открытого ключа для вывода на бумажный носитель;
- Список сертификатов открытого ключа пользователя УЦ и их статус;
- Список запросов на сертификаты открытых ключей пользователя УЦ и их статус;
- Список запросов на аннулирование (отзыв), приостановление и возобновление действия сертификатов открытых ключей пользователя УЦ и их статус.

10.3. Организационные меры защиты информации

10.3.1. Предъявляемые требования к персоналу Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет.

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

10.3.2. Профессиональная переподготовка и повышение квалификации персонала

Профессиональная переподготовка персонала Удостоверяющего Центра не осуществляется.

Сотрудники Удостоверяющего Центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

10.3.3. Организация сменной работы

Деятельность Удостоверяющего Центра по работе с пользователями УЦ в части приема заявлений в бумажной форме и изготовления сертификатов открытых ключей организована в одну рабочую смену с 9.00 до 18.00 в будние дни.

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

10.3.4. Организация доступа персонала к документам и документации

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

10.3.5. Охрана здания и помещений

Удостоверяющий Центр имеет собственную (привлекаемую) службу охраны здания и помещений, обеспечивающую:

- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) Удостоверяющего Центра;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

10.4. Юридические меры защиты информации

Удостоверяющий Центр имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг (см. 2.2).

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

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

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

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

Пользователям УЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые Удостоверяющим Центром в объеме прав согласно разделу 3.2 настоящего Регламента.

11. Взаимодейсвтие Удостоверяющего центра с Уполномоченным федеральным органом исполнительной власти в области применения ЭЦП

Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица Удостоверяющего центра для заверения от имени Удостоверяющего центра сертификатов открытых ключей обязан предоставить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица Удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе.

Ответственный сотрудник Удостоверяющего центра, входящий в состав Службы Администрирования, распечатывает сертификат ключа подписи уполномоченного лица Удостоверяющего центра на бумажном носителе. Данный сертификат визируются собственноручной подписью уполномоченного лица Удостоверяющего центра и руководителя и заверяется печатью Удостоверяющего центра.

Ответственный сотрудник Удостоверяющего центра, входящий в состав Службы Администрирования записывает сертификат ключа подписи уполномоченного лица Удостоверяющего центра в электронной форме на сменный носитель (дискета, CD-ROM).

Сертификат ключа подписи уполномоченного лица Удостоверяющего центра в электронной и бумажной форме, а также заверенную руководителем копию распорядительного документа о назначении уполномоченного лица Удостоверяющего центра, направляются сопроводительным письмом в адрес Уполномоченного федерального органа исполнительной власти в области применения ЭЦП.

С информацией из Единого государственного реестра сертификатов уполномоченных лиц Удостоверяющих центров, а также с изменениями в порядке регистрации сертификатов уполномоченных лиц Удостоверяющих центров, можно ознакомиться на сайте Уполномоченного федерального органа исполнительной власти в области применения ЭЦП – http://www.reestr-pki.ru.

Приложение 1. Сокращения

РФ – Российская Федерация;
СОС – список отозванных сертификатов;
УЦ – удостоверяющий центр;
ЦР – центр регистрации;
ЦС – центр сертификации;
ЭД – электронный документооборот;
ЭЦП – электронная цифровая подпись.

Приложение 2. Термины и определения

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Закрытый ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и/или шифрования данных.

Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата.

Запрос на отзыв сертификата

Сообщение, содержащее необходимую информацию для отзыва сертификата.

Идентификация

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

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключевая пара

Открытый и закрытый ключи.

Ключевой носитель

Носитель, содержащий один или несколько ключей.

Компрометация ключа

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

Открытый ключ

Криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы и предназначен для проверки электронной цифровой подписи и шифрования. При этом открытый ключ не позволяет вычислить закрытый ключ.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Сертификат

Цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью его издателя. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 и рекомендациях IETF 1999 года RFC 2459.

Список отозванных сертификатов

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

Средства электронной цифровой подписи

Аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи

подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Центр сертификации

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

Центр регистрации

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

Приложение 3. Структуры записей аудита

Структура записи аудита модуля политики службы сертификации ЦС

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

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

Все поля в записи журнала аудита разделяются знаком табуляции.

Структура записи аудита ПО Центра Регистрации

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

Структура записи аудита Windows 2000 Server

Поле	Описание
Дата	Дата, когда произошло данное событие.
Время	Локальное время, когда произошло данное событие.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного

	процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода. (Олицетворение происходит в тех случаях, когда в Windows 2000 один процесс присваивает атрибуты безопасности другого процесса.)
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера Windows 2000.
Код события	Число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Например, 6005 — это идентификатор события, которое происходит при запуске службы ведения журналов событий. Соответственно, в начале описания этого события находится строка «Запущена служба журнала событий». Код события и имя источника записи могут использоваться представителями группы поддержки программного продукта для устранения неполадок.
Источник	Программа, занесшая событие. Это может быть как имя программы (например, «SQL Server»), так и название компонента системы или большого приложения (например, название драйвера). Например, «Elnkii» означает драйвер EtherLink II.
Тип	Уровень важности события: «Ошибка», «Уведомление» или «Предупреждение» в журналах системы и приложений; «Аудит успехов» или «Аудит отказов» в журнале безопасности. В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория события в зависимости от источника события. Это сведения используются преимущественно в журнале безопасности. Например, для аудита событий безопасности категория соответствует одному из типов событий, для которых в групповой политике может быть включен аудит успехов или отказов.

Структура записи аудита MS Internet Information Server (IIS)

Поле	Обозначение в журнале аудита	Описание
Дата	`date`	Дата возникновения события.
Время	`time`	Время возникновения события.
IP-адрес клиента	`c-ip`	IP-адрес клиента, получившего доступ к серверу.
Имя пользователя	`c-username`	Имя пользователя, получившего доступ к серверу. Это не относится к анонимным пользователям, которые обозначаются черточками.
Имя службы	`s-sitename`	Служба Интернета, выполнявшаяся на компьютере клиента, и номер экземпляра.
Имя сервера	`s-computername`	Имя сервера, на котором была создана запись журнала.
Адрес IP сервера	`s-ip`	IP-адрес сервера, на котором была создана запись журнала.
Метод	`cs-method`	Действие, которое пытался выполнить клиент (например, метод GET).

Ресурс URI	cs-uri-stem	Ресурс, к которому было выполнено обращение, например Default.htm.
Запрос URI	cs-uri-query	Запрос, который пытался выполнить клиент.
Состояние протокола	sc-status	Состояние действия (в терминах HTTP).
Состояние Win32	sc-win32-status	Состояние действия (в терминах Windows 2000).
Передано байт	sc-bytes	Число байт, отправленных сервером.
Получено байт	cs-bytes	Число байт, полученных сервером.
Порт сервера	s-port	Номер порта, к которому подключен клиент.
Заняло времени	time-taken	Время, которое заняло выполнение действия.
Версия протокола	cs-protocol	Версия протокола (HTTP, FTP), используемого клиентом. Для протокола HTTP это либо HTTP 1.0, либо HTTP 1.1.
Агент пользователя	cs(User-Agent)	Обозреватель, используемый клиентом.
Объект Cookie	cs(Cookie)	Содержимое отправленного или полученного модуля настройки клиента (cookie) (если имеется).
Источник ссылки	cs(Referer)	Предыдущий просмотренный пользователем узел. На этом узле содержалась ссылка на данный узел.

Все поля в записи журнала аудита разделяются пробелами.

Структура записи аудита SQL 2000 Server

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

Все поля в записи журнала аудита разделяются пробелами.