

ЗАКРЫТОЕ
АКЦИОНЕРНОЕ
ОБЩЕСТВО

350063, г. Краснодар
ул. Комсомольская, 40
orbital@orbitacom.ru
www.orbitacom.ru



УТВЕРЖДАЮ
Генеральный директор
ЗАО «Орбита»



И.В. Алексеев

2010г.

Регламент Удостоверяющего центра

Закрытого акционерного общества «Орбита»

СОГЛАСОВАНО
Начальник УЦ ЗАО «Орбита»

 / А.В. Ляцев /

« 24 » мая 2010 г.

г. Краснодар, 2010г.

Оглавление

Оглавление	2
1 Введение	6
1.1 Сведения об удостоверяющем центре	6
1.2 Идентификация Регламента	7
1.3 Статус Регламента.....	7
1.4 Присоединение к Регламенту	7
1.5 Публикация Регламента.....	7
1.6 Область применения Регламента	8
1.7 Срок действия Регламента	8
1.8 Контактная информация	8
2 Общие положения.....	8
2.1 Назначение Удостоверяющего Центра.....	8
2.2 Услуги, предоставляемые Удостоверяющим Центром	8
2.3 Пользователи услуг Удостоверяющего Центра	9
2.4 Разрешение споров	9
2.4.1 Процедура экспертизы	10
2.4.2 Бремя доказывания при разрешении споров.....	10
2.5 Ответственность	10
2.6 Прекращение деятельности	10
2.7 Порядок утверждения и внесения изменений в Регламент	10
3 Права.....	11
3.1 Права Удостоверяющего Центра	11
3.2 Права пользователей УЦ.....	12
4 Обязательства	13
4.1 Обязательства Удостоверяющего Центра.....	13
4.1.1 Ключ подписи уполномоченного лица Удостоверяющего Центра.....	13
4.1.2 Синхронизация времени	13
4.1.3 Регистрация пользователей УЦ.....	13
4.1.4 Изготовление закрытых ключей пользователей УЦ.....	14
4.1.5 Изготовление сертификатов ключей подписи	14
4.1.6 Аннулирование (отзыв) сертификатов ключей подписи	14
4.1.7 Приостановление действия сертификатов ключей подписи	14
4.1.8 Возобновление действия сертификатов ключей подписи	15
4.1.9 Уведомления	15
4.1.10 Реестр сертификатов ключей подписи.....	16
4.1.11 Прочие обязательства	16
4.2 Обязательства пользователей УЦ	16
4.2.1 Обязанности лиц, проходящих процедуру регистрации	16

4.2.2	Обязанности владельцев закрытых ключей	16
4.2.3	Обязанности владельца сертификата открытого ключа.....	17
4.2.4	Обязанности пользователей сертификатов ключей подписи.....	17
5	Политика конфиденциальности	17
5.1	Типы конфиденциальной информации	17
5.2	Типы информации, не являющейся конфиденциальной	17
5.3	Исключительные полномочия официальных лиц	18
6	Процедуры и механизмы	18
6.1	Процедура регистрации пользователей УЦ	18
6.1.1	Заявление на изготовление сертификата ключа подписи.....	18
6.1.2	Идентификация пользователя УЦ	19
6.2	Регистрация пользователя УЦ в централизованном режиме.....	19
6.3	Регистрация пользователя УЦ в распределенном режиме.....	19
6.4	Изготовление закрытых ключей и сертификата открытого ключа в централизованном режиме.....	20
6.5	Изготовление закрытых ключей и сертификата открытого ключа в распределенном режиме.....	21
6.5.1	Заявление на изготовление сертификата ключа подписи в электронной форме	22
6.6	Идентификация зарегистрированного пользователя.....	22
6.7	Аутентификация зарегистрированного пользователя.....	22
6.7.1	Очная аутентификация зарегистрированного пользователя	22
6.7.2	Удаленная аутентификация зарегистрированного пользователя.....	22
6.7.3	Аутентификация зарегистрированного пользователя по сертификату открытого ключа	23
6.7.4	Идентификация владельца сертификата открытого ключа	23
6.8	Аннулирование (отзыв) сертификата открытого ключа	23
6.9	Приостановление действия сертификата открытого ключа	23
6.9.1	Заявление на приостановление действия сертификата открытого ключа в бумажной форме	24
6.10	Возобновление действия сертификата открытого ключа	24
6.10.1	Заявление на возобновление действия сертификата открытого ключа в бумажной форме	24
6.11	Процедура подтверждения электронной цифровой подписи с использованием сертификата открытого ключа.....	24
6.12	Процедура подтверждения электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в сертификате открытого ключа	26
6.13	Механизм доказательства обладания закрытым ключом, соответствующим открытому ключу	27
7	Вознаграждение Удостоверяющего центра. Сроки и порядок расчетов	27
8	Дополнительные положения	27
8.1	Идентифицирующие данные уполномоченного лица Удостоверяющего Центра ...	27
8.2	Сроки действия ключей уполномоченного лица Удостоверяющего Центра	28
8.3	Требования к средствам электронной цифровой подписи пользователей УЦ.....	28

8.4	Сроки действия закрытых ключей и сертификатов ключей подписи владельцев сертификатов ключей подписи	29
8.5	Закрытые ключи и сертификат открытого ключа.....	29
8.6	Меры защиты закрытых ключей	29
8.7	Копия сертификата открытого ключа электронной форме.....	30
8.8	Копия сертификата открытого ключа на бумажном носителе.....	30
8.9	Архивное хранение документированной информации.....	30
8.9.1	Состав архивируемых документов	30
8.9.2	Архивохранилище	30
8.9.3	Уничтожение архивных документов	31
8.10	Смена ключей уполномоченного лица Удостоверяющего Центра	31
8.10.1	Плановая смена ключей уполномоченного лица Удостоверяющего Центра ...	31
8.10.2	Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра	31
9	Структуры сертификатов и списков отозванных сертификатов	32
9.1	Структура сертификата открытого ключа, изготавливаемого Удостоверяющим Центром в электронной форме	32
9.1.1	Базовые поля сертификата открытого ключа	32
9.1.2	Дополнения сертификата.....	32
9.1.3	Объектные идентификаторы алгоритма.....	32
9.1.4	Формы имени.....	33
9.1.5	Ограничения на имена	33
9.2	Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме	33
9.2.1	Дополнения СОС.....	33
10	Программные и технические средства обеспечения деятельности Удостоверяющего Центра	34
10.1	Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра.....	34
10.2	Технические средства обеспечения работы ПК УЦ	35
10.3	Программные и программно-аппаратные средства защиты информации.....	35
10.4	Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций Удостоверяющего Центра	36
10.5	Перечень данных программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра, подлежащих резервному копированию.....	36
11	Обеспечение безопасности	37
11.1	Инженерно-технические меры защиты информации	37
11.1.1	Размещение технических средств Удостоверяющего Центра.....	37
11.1.2	Физический доступ в помещения	37
11.1.3	Электроснабжение и кондиционирование воздуха	37
11.1.4	Предупреждение и защита от возгорания.....	38
11.1.5	Хранение документированной информации	38
11.1.6	Уничтожение документированной информации	38

11.2	Программно-аппаратные меры защиты информации.....	38
11.2.1	Организация доступа к техническим средствам Удостоверяющего Центра	38
11.2.2	Организация доступа к программным средствам Удостоверяющего Центра...	38
11.2.3	Контроль целостности программного обеспечения	39
11.2.4	Контроль целостности технических средств.....	39
11.3	Организационные меры защиты информации	40
11.3.1	Предъявляемые требования к персоналу Удостоверяющего Центра	40
11.3.2	Профессиональная переподготовка и повышение квалификации персонала Удостоверяющего центра	40
11.3.3	Организация сменной работы Удостоверяющего центра	40
11.3.4	Организация доступа персонала к документам и документации Удостоверяющего центра	40
11.4	Юридические меры защиты информации.....	40
12	Взаимодействие Удостоверяющего центра с Уполномоченным федеральным органом исполнительной власти в области применения ЭЦП.	40
13	Формирование объектных идентификаторов областей применения сертификатов открытых ключей	41
	Приложение 1.	42
	Приложение 2.	43

1 Введение

1.1 Сведения об удостоверяющем центре

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего Центра (УЦ) Закрытого акционерного общества «Орбита» (далее по тексту – ЗАО «Орбита»), 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.

Закрытое акционерное общество «Орбита», в состав которого входит Удостоверяющий Центр, зарегистрировано на территории Российской Федерации в городе Краснодаре. Свидетельство о регистрации: регистрационный № 14272, выдано 07.09.2000г. Регистрационной палатой Мэрии г. Краснодара, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1022301424507 от 23.07.2002 г

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

Лицензия ФСБ России № 719/Р от 27.12.2007 г. на право осуществлять деятельность по распространению шифровальных (криптографических) средств.

Лицензия ФСБ России № 719/Т от 27.12.2007 г. на право осуществлять деятельность по техническому обслуживанию шифровальных (криптографических) средств.

Лицензия ФСБ России № 719/У от 27.12.2007 г. на право осуществлять предоставление услуг в области шифрования информации.

Лицензия ФСБ России № 5077П от 07.02.2008 г. на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Лицензия Федеральной службы по техническому и экспортному контролю №0055 от 20.02.2003г (срок действия продлен 16.02.2008) на деятельность по технической защите конфиденциальной информации.

Реквизиты ЗАО "Орбита":

Полное наименование: Закрытое акционерное общество «Орбита»

Юридический адрес: 350063, г. Краснодар, ул. Комсомольская, 40

Фактический адрес: 350063, г. Краснодар, ул. Комсомольская, 40

Банковские реквизиты (наименование банка, БИК, ИНН, р/с, к/с):

- Краснодарский филиал Банка «ВОЗРАЖДЕНИЕ» (ОАО)

БИК 040349994

ИНН 2309072734

Р/с 40702810706500140519

К/с 30101810300000000994

ИНН/КПП: 2309072734/230901001

ОГРН: 1022301424507

Код по ОКВЭД: 45.31; 72.10; 72.20; 72.30; 72.40; 72.50; 72.60

Код по ОКПО: **55103655**

Контактные телефоны, факс, адрес электронной почты:

тел. (861) 268-67-67; факс. (861) 268-67-67 e-mail: ca@orbitacom.ru

1.2 Идентификация Регламента

Наименование документа: «Регламент Удостоверяющего Центра Закрытого акционерного общества «Орбита» Редакция №2

1.3 Статус Регламента

Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

Регламент разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

1.4 Присоединение к Регламенту

Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр Заявления о присоединении к Регламенту.

С момента регистрации Заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившемся к Регламенту и является Стороной Регламента.

Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления о присоединении к Регламенту.

Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении в реестре Удостоверяющего центра. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

1.5 Публикация Регламента

Настоящий Регламент распространяется:

- **в электронной форме:**

1.1. через E-mail от отправителя **ca@orbitacom.ru**

1.2. из репозитория Владельца УЦ по адресу www.orbitacom.ru.

Копии Регламента, предназначенные для распространения в электронной форме распространяются в виде двух файлов, один из которых содержит электронный образ Регламента в формате RTF (Rich Text Format), а другой - электронную цифровую подпись руководителя Удостоверяющего Центра файла электронного образа Регламента.

- **в бумажной форме:**

Лично в руки заявителю, при подаче Заявления о присоединении к Регламенту (за вознаграждение, установленное настоящим Регламентом)

Служба регистрации Удостоверяющего центра расположена по адресу 350063, г. Краснодар, ул. Комсомольская, 40.

1.6 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.

1.7 Срок действия Регламента

Настоящий Регламент вступает в силу с «01» июля 2010г. Срок действия Регламента – 5 лет.

Если Удостоверяющий Центр официально не уведомит пользователей УЦ о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 5 лет. Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе публикации Регламента

1.8 Контактная информация

Закрытое акционерное общество «Орбита»,
Адрес: 350063, г. Краснодар, ул. Комсомольская, 40
Тел:г.Краснодар: +7(861) 262-97-98
г.Ростов-на-дону: +7(863) 250-91-00
г.Ставрополь: +7(8652) 95-16-16

Web сайт : http://www.orbitacom.ru/services/service_uc.

e-mail: ca@orbitacom.ru

2 Общие положения

2.1 Назначение Удостоверяющего Центра

Удостоверяющий Центр предназначен для обеспечения участников информационных систем средствами и спецификациями для использования сертификатов ключей подписи 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 ключей подписи пользователей УЦ в электронной форме;

3. изготовление копии сертификатов ключей подписи 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 ключей подписи пользователей УЦ;
6. предоставление копий сертификатов ключей подписи в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
7. аннулирование (отзыв) сертификатов ключей подписи по обращениям владельцев сертификатов ключей подписи;
8. приостановление и возобновление действия сертификатов ключей подписи по обращениям владельцев сертификатов ключей подписи;
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;

2.3 Пользователи услуг Удостоверяющего Центра

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

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

Группа 2. зарегистрированные на УЦ лица, являющиеся владельцами сертификатов ключей подписи.

Зарегистрированные на УЦ лица, являющиеся владельцами сертификатов ключей подписи, 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 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.

2.4 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 г.Краснодара в соответствии с действующим законодательством Российской Федерации.

2.4.1 Процедура экспертизы

При разрешении в претензионном порядке споров, связанных с использованием ЭЦП, в обязательном порядке производится экспертиза, для осуществления которой привлекается Удостоверяющий центр, зарегистрировавший открытый ключ ЭЦП, в отношении которой возник спор.

Экспертиза проводится в порядке, установленном УЦ или соответствующим соглашением сторон.

2.4.2 Бремя доказывания при разрешении споров

В случае возникновения споров о наличии ЭЦП под электронным документом бремя доказывания лежит на Стороне, не соглашающейся с наличием ЭЦП.

В случае возникновения споров о факте внесения изменений в электронный документ после его подписания ЭЦП бремя доказывания лежит на Стороне, утверждающей, что в данный электронный документ были внесены изменения после его подписания ЭЦП.

В случае возникновения споров о факте получения одной из Сторон какого-либо электронного документа, подписанного ЭЦП, от другой Стороны, бремя доказывания лежит на Стороне, не соглашающейся с фактом получения кем-либо электронного документа, подписанного ЭЦП.

2.5 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.

2.6 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 ключей подписи, могут передаваться в другой, действующий на момент передачи Удостоверяющий центр по согласованию с владельцами сертификатов.

2.7 Порядок утверждения и внесения изменений в Регламент

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

Внесение изменений (дополнений) в Регламент, включая приложения и дополнения к нему, производится Удостоверяющим центром в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на сайте Удостоверяющего центра.

Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении одного месяца с даты размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра.

Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение договора присоединения к Регламенту.

Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью

3 Права

3.1 Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

1. Предоставлять копии сертификатов ключей подписи 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 ключей подписи в электронной форме, находящихся в реестре Удостоверяющего Центра;

3. Отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на изготовление ключа подписи, с указаниями причин отказа; 4. Отказать в изготовлении ключей не зарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, с указанием причин отказа

4. Отказать в изготовлении сертификата открытого ключа зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата открытого ключа, с указанием причин отказа;

5. 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;

6. 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;

7. 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;

8. Приостановить действие сертификата открытого ключа пользователя УЦ, с уведомлением владельца приостановленного сертификата открытого ключа и указанием обоснованных причин.

3.2 Права пользователей УЦ

Пользователи сертификатов ключей подписи Группы 1 имеют следующие права:

1. Получить список аннулированных (отозванных) и приостановленных сертификатов ключей подписи, 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 ключей подписи 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 ключей подписи, изготовленный Удостоверяющим Центром, для проверки статуса сертификатов ключей подписи.
7. Обратиться в Удостоверяющий Центр для внесения в реестр Удостоверяющего Центра регистрационной информации о пользователе, с целью в дальнейшем стать владельцем сертификата открытого ключа;
8. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных цифровых подписей в документах, представленных в электронной форме;
9. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах открытых ключей;
10. Обратиться в Удостоверяющий Центр на предмет получения (приобретения) средства электронной цифровой подписи;
11. Сформировать закрытые ключи на своем рабочем месте с использованием средства ЭЦП и программных средств, предоставляемых Удостоверяющим Центром. Передать запрос на изготовление сертификата ключа подписи в электронном виде на Удостоверяющий центр.

Пользователи сертификатов ключей подписи Группы 2 имеют 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 ключей подписи в электронной форме из Реестра сертификатов ключей подписи Удостоверяющего Центра;

7. 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

4 Обязательства

4.1 Обязательства Удостоверяющего Центра

4.1.1 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 ключей подписи и списков отозванных сертификатов.

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

4.1.2 Синхронизация времени

Удостоверяющий Центр организует работу своих Служб по GMT (Greenwich Mean Time) с учетом часового пояса г. Москвы. Удостоверяющий Центр обязан синхронизировать по времени все программные и технические средства обеспечения деятельности по назначению.

4.1.3 Регистрация пользователей УЦ

Удостоверяющий Центр обеспечивает регистрацию пользователей УЦ по заявлениям на изготовление ключа подписи в соответствии с порядком регистрации, изложенным в настоящем Регламенте. Удостоверяющий Центр обязан обеспечить уникальность регистрационной информации пользователей УЦ, заносимой в реестр Удостоверяющего Центра и используемой для идентификации владельцев сертификатов ключей подписи.

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

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

4.1.4 Изготовление закрытых ключей пользователей УЦ

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

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

Удостоверяющий Центр обязан выполнять процедуру создания ключей и запись ключей подписи на отчуждаемые носители только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством Российской Федерации.

Допускается изготовление закрытых ключей регистрирующимся лицом либо пользователем УЦ самостоятельно, на своем рабочем месте, с использованием программных средств, предоставленных Удостоверяющим центром. Владелец ключа обязан использовать средства электронной цифровой подписи, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Владелец закрытого ключа обязан обеспечить сохранение в тайне изготовленного закрытого ключа.

4.1.5 Изготовление сертификатов ключей подписи

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 ключей подписи пользователей УЦ.

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

4.1.6 Аннулирование (отзыв) сертификатов ключей подписи

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

Удостоверяющий Центр обязан аннулировать (отозвать) сертификат открытого ключа по факту отзыва доверенности, в случае если владелец сертификата представляет интересы юридического лица.

Удостоверяющий Центр обязан в течение 24 часов с момента регистрации заявления на отзыв сертификата или уведомления об отзыве доверенности занести сведения об аннулированном (отозванном) сертификате в список отозванных сертификатов с указанием даты и времени занесения и причины отзыва.

4.1.7 Приостановление действия сертификатов ключей подписи

Удостоверяющий Центр обязан приостановить действие сертификата 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.

4.1.8 Возобновление действия сертификатов ключей подписи

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.

4.1.9 Уведомления

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 информацией о выпущенном сертификате открытого ключа с адреса отправителя sa@orbitacom.ru.

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

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 репозитории Владельца УЦ по адресам, указанным в изготовленных сертификатах ключа подписи.

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 репозитория Удостоверяющего Центра в издаваемые сертификаты открытых ключей пользователей УЦ.

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 репозитории Владельца УЦ по адресам, указанным в изготовленных сертификатах ключа подписи.

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.

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 репозитории Владельца УЦ по адресам, указанным в изготовленных сертификатах ключа подписи. 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.

4.1.10 Реестр сертификатов ключей подписи

Удостоверяющий Центр обязан вести реестр всех изготовленных сертификатов ключей подписи пользователей УЦ в течение установленного срока хранения. Реестр сертификатов ключей подписи ведется в электронном виде.

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

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

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

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

4.1.11 Прочие обязательства

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

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.

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;
- 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;
- 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; .

4.2.4 Обязанности пользователей сертификатов ключей подписи

Перед тем как использовать сертификат открытого ключа, изготовленный Удостоверяющим Центром, пользователь сертификата Группы 1 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.

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 ключей подписи пользователей УЦ и/или формирования закрытых и открытых ключей пользователей УЦ с записью их на ключевой носитель.

6.1.1 Заявление на изготовление сертификата ключа подписи

Лицо (заявитель), желающее пройти процедуру регистрации на Удостоверяющем Центре, должно подать заявление на изготовление сертификата ключа подписи в простой письменной форме, заверенное собственноручной подписью, в Службу Регистрации УЦ. В случае прохождения процедуры регистрации пользователя УЦ в распределенном режиме, заявление заверяется нотариально.

Заявление должно содержать следующие обязательные реквизиты:

Для физического лица:

Идентификационные данные, включающие:

- Фамилию, имя и отчество;
- Адрес электронной почты.

Паспортные данные:

- Вид документа;
- Серия паспорта;
- Номер паспорта;
- Кем выдан;
- Когда выдан.

Данные об областях использования сертификата ключа подписи.

Данные для удаленной идентификации (ключевая фраза) до 64 символов.

Данные указанные в заявке заверяются собственноручной подписью заявителя,

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.

Формы заявлений на изготовление сертификата ключа подписи для различных информационных систем публикуются на сайте http://www.orbitacom.ru/servises/servise_uc Удостоверяющего центра или предоставляется Удостоверяющим центром по запросу на адрес электронной почты ca@orbitacom.ru

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 изготовление сертификата ключа подписи (см. раздел 6.1.1 настоящего Регламента).

6.2 Регистрация пользователя УЦ в централизованном режиме

Регистрация пользователя УЦ осуществляется администратором Удостоверяющего Центра на основании заявления на изготовление сертификата ключа подписи при личном прибытии лица, проходящего процедуру регистрации, в офис Удостоверяющего Центра, расположенный по адресу: 350063, г. Краснодар, ул. Комсомольская, 40.

Соискатель на получение ЭЦП заверяет заявление на изготовление сертификата ключа подписи собственноручной подписью и передает заявление вместе с необходимыми приложениями в Удостоверяющий Центр.

Идентификация соискателя проходящего регистрацию выполняется путем предоставления им паспорта либо другого документа удостоверяющего личность.

В случае отказа в регистрации заявление на изготовление сертификата ключа подписи вместе с приложениями возвращается заявителю.

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

6.3 Регистрация пользователя УЦ в распределенном режиме

Регистрация пользователя УЦ в распределенном режиме осуществляется администратором УЦ на основании нотариально заверенного заявления на изготовление сертификата ключа подписи лица, проходящего процедуру регистрации, поступившего в офис Удостоверяющего Центра, расположенный по адресу 350063, г. Краснодар, ул. Комсомольская,

40, и на основании заявления на изготовление ключа подписи в электронной форме, поступившего в Удостоверяющий Центр по каналам связи или на отчуждаемом носителе.

Идентификация лица, проходящего процедуру регистрации, выполняется нотариусом в процессе совершения нотариальных действий по заверению заявления на изготовление сертификата ключа подписи.

Администратор УЦ выполняет процедуру проверки соответствия идентификационных данных, поступивших в запросе на изготовление ключа подписи в электронной форме и в заявлении на изготовление сертификата ключа подписи в бумажной форме.

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, а также списки отозванных сертификатов в электронной форме Удостоверяющего Центра.

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

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

Заявление на изготовление сертификата ключа подписи рассматривается в УЦ в течение 2 рабочих дней с момента его поступления.

В случае отказа в регистрации заявление на изготовление сертификата ключа подписи заявление вместе с приложениями заявителю не возвращается.

Официальным уведомлением пользователя УЦ об отказе в регистрации является отправка электронного почтового сообщения с адреса отправителя sa@orbitacom.ru на электронный адрес, указанный в заявлении на изготовление сертификата ключа подписи.

При принятии положительного решения, администратор УЦ выполняет действия по занесению регистрационной информации в реестр Удостоверяющего Центра. Производит изготовление сертификата ключа подписи.

Официальным уведомлением пользователя УЦ о регистрации является отправка электронного почтового сообщения с адреса отправителя sa@orbitacom.ru на электронный адрес, указанный в заявлении на изготовление сертификата ключа подписи.

Отсутствие в течение 10 рабочих дней официального уведомления пользователя УЦ о регистрации является официальным отказом в регистрации.

6.4 Изготовление закрытых ключей и сертификата открытого ключа в централизованном режиме.

Изготовление закрытых ключей и сертификата открытого ключа в централизованном режиме осуществляется Удостоверяющим Центром на основании заявления на изготовление сертификата ключа подписи зарегистрированного пользователя УЦ. Заявление на изготовление сертификата ключа подписи подается заявителем в УЦ лично.

Изготовление ключей выполняется администратором УЦ на специализированном рабочем месте 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 Удостоверяющим центром;
- 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 фиксируется в акте выполненных работ прилагаемому к договору присоединения к регламенту УЦ ЗАО «Орбита»

Срок рассмотрения заявления на изготовление сертификата открытого ключа составляет 2 часа с момента его поступления в УЦ.

По окончании процедуры изготовления ключей зарегистрированному пользователю Удостоверяющего Центра выдаются:

- ключ, записанный на ключевой носитель;
- сертификат открытого ключа в электронной форме, соответствующий закрытому ключу;
- копия сертификата открытого ключа на бумажном носителе, по форме определенной настоящим Регламентом;
- сертификат открытого ключа в электронной форме уполномоченного лица Удостоверяющего Центра;

Указанные выше данные, передаваемые зарегистрированному пользователю УЦ в электронной форме, записываются в виде файлов на съемный машинный носитель.

6.5 Изготовление закрытых ключей и сертификата открытого ключа в распределенном режиме.

Изготовление сертификата ключа подписи в распределенном режиме осуществляется администратором УЦ на основании нотариально заверенного заявления на изготовление сертификата ключа подписи и заявления на изготовление сертификата ключа подписи в электронном виде.

Заявление на изготовление сертификата ключа подписи в бумажной и электронной форме подается зарегистрированным пользователем УЦ в Удостоверяющий центр посредством почтовой или курьерской связи. Заявление на изготовление ключа подписи в электронной форме передается в УЦ по каналам связи, способами, определяемыми Удостоверяющим центром.

Изготовление закрытых ключей осуществляется регистрирующимся лицом либо пользователем УЦ самостоятельно, на своем рабочем месте, с использованием программных средств, предоставленных Удостоверяющим центром. Владелец ключа обязан использовать средств электронной цифровой подписи, сертифицированные в соответствии с действующим законодательством Российской Федерации.

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

В случае отказа в изготовлении сертификата ключа подписи заявление на изготовление сертификата ключа подписи вместе с приложениями заявителю не возвращается.

Официальным уведомлением пользователя УЦ об отказе в изготовлении сертификата ключа подписи является отправка электронного почтового сообщения с адреса отправителя sa@orbitacom.ru на электронный адрес, указанный в заявлении на изготовление сертификата ключа подписи.

При принятии положительного решения, администратор УЦ выполняет действия по изготовлению сертификата ключа подписи. Официальным уведомлением пользователя УЦ о изготовлении сертификата ключа подписи является отправка электронного почтового сообщения с адреса отправителя sa@orbitacom.ru на электронный адрес, указанный в заявлении на изготовление сертификата ключа подписи.

Изготовленный сертификат открытого ключа в электронной форме, заверенный электронной цифровой подписью уполномоченного лица Удостоверяющего Центра, предоставляется его владельцу путем отправки по электронной почте с адреса sa@orbitacom.ru в виде прикрепленного файла архива формата сжатия данных ZIP, содержащего изготовленный сертификат в электронной форме.

Копия сертификата открытого ключа на бумажном носителе предоставляется его владельцу при личном обращении в УЦ, либо посредством почтовой или курьерской связи.

6.5.1 Заявление на изготовление сертификата ключа подписи в электронной форме

Заявление на изготовление сертификата открытого ключа в электронной форме представляет собой электронный документ формата PKCS#7, содержащий в качестве данных запрос на сертификат в формате PKCS#10

Владельцы сертификатов ключей подписи подписывают заявление на изготовление сертификата открытого ключа в электронной форме электронной цифровой подписью с использованием закрытого ключа подписи, владельцем которых является заявитель. В качестве закрытого ключа подписи должен использоваться закрытый ключ, до окончания срока действия которого, на момент поступления заявления в УЦ, остается не менее 1 календарного месяца.

6.6 Идентификация зарегистрированного пользователя

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

6.7 Аутентификация зарегистрированного пользователя

6.7.1 Очная аутентификация зарегистрированного пользователя

Очная аутентификация зарегистрированного пользователя УЦ выполняется по паспорту, предъявляемому лично.

6.7.2 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 изготовление сертификата ключа подписи.

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

6.7.3 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 6.11 настоящего Регламента).

6.7.4 Идентификация владельца сертификата открытого ключа

Владелец сертификата открытого ключа идентифицируется по значениям атрибутов поля Subject сертификата открытого.

6.8 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 бумажной форме в УЦ.

Заявление на отзыв сертификата открытого ключа в бумажной форме подается заявителем в УЦ лично, либо посредством почтовой или курьерской связи.

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

После аннулирования (отзыва) сертификата открытого ключа его владельцу направляется официальное уведомление.

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.

К заявлению прилагается ксерокопия сертификата ключа подписи на бумажном носителе, заверенная собственноручной подписью владельца ключа.

6.9 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 бумажной форме в Службу Безопасности УЦ.

Заявление на приостановление действия сертификата открытого ключа в бумажной форме подается заявителем в УЦ лично, либо посредством почтовой или курьерской связи.

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

После приостановления действия сертификата открытого ключа его владельцу направляется официальное уведомление.

6.9.1 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.

6.10 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 бумажной форме в УЦ.

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

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

После возобновления действия сертификата открытого ключа его владельцу направляется официальное уведомление.

6.10.1 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.

6.11 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 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 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 10 рабочих дней с момента его поступления в 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 администратора 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 администратора 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.

6.12 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 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 10 рабочих дней с момента его поступления в 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 уполномоченного лица 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 уполномоченного лица 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.

6.13 Механизм доказательства обладания закрытым ключом, соответствующим открытому ключу

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

7 Вознаграждение Удостоверяющего центра. Сроки и порядок расчетов

Вознаграждение УЦ по услугам, предоставляемым в соответствии с п.п 6.1-6.13 Регламента, устанавливается в соответствии с прайс-листом, утверждаемым приказом генеральным директором ЗАО «Орбита».

Действующий прайс-лист можно получить с WEB сервера по адресу: http://www.orbitacom.ru/servises/service_ус или получить в офисе УЦ.

Пользователь УЦ оплачивает аванс в размере 100% стоимости услуг, оказываемых Удостоверяющим Центром.

8 Дополнительные положения

8.1 Идентифицирующие данные уполномоченного лица Удостоверяющего Центра

Уполномоченное лицо Удостоверяющего Центра идентифицируется по следующим данным:

CN = SFD Class 1 CA

OU = CA Orbita

O = LJSC Orbita
L = Krasnodar
S = Krasnodar region
C = RU
E = ca@orbitacom.ru

8.2 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 с момента начала срока действия 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 7 лет.

8.3 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. В качестве средства электронной цифровой подписи пользователи должны использовать сертифицированные в соответствии с правилами сертификации средства криптографической защиты информации по уровню защиты не ниже «KC1».

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

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.

8.4 Сроки действия закрытых ключей и сертификатов ключей подписи владельцев сертификатов ключей подписи

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 ключей подписи 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 Таблице 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.	Пользователь Центра Регистрации	1.2.643.2.2.34.6	1 год 3 месяца
2.	Временный доступ к Центру Регистрации	1.2.643.2.2.34.2	1 месяц
3.	Защищенная электронная почта	1.3.6.1.5.5.7.3.4	5 лет
4.	Проверка подлинности клиента	1.3.6.1.5.5.7.3.2	1 год

8.5 Закрытые ключи и сертификат открытого ключа

Закрытые ключи и сертификат открытого ключа предназначены для использования в соответствии со сведениями, указанными в сертификате в областях использования.

8.6 Меры защиты закрытых ключей

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 владелец 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.

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.

8.7 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.

8.8 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.

8.9 Архивное хранение документированной информации

8.9.1 Состав архивируемых документов

Архивированию подлежат следующая документированная информация:

- Реестр сертификатов ключей подписи 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 сертификатов ключей подписи пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов ключей подписи;
- заявления на приостановление действия сертификатов ключей подписи;
- заявления на возобновление действия сертификатов ключей подписи;
- служебные документы Удостоверяющего Центра.

8.9.2 Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации. Сертификат ключа подписи в форме документа на

бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

8.9.3 Уничтожение архивных документов

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

8.10 Смена ключей уполномоченного лица Удостоверяющего Центра

8.10.1 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 3 месяцев 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.

8.10.2 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.

9 Структуры сертификатов и списков отозванных сертификатов

9.1 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.

9.1.1 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 ключей подписи Удостоверяющего Центра

9.1.2 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 ключей подписи, изданных Удостоверяющим Центром

KeyUsage: Назначение ключа

9.1.3 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

9.1.4 Формы имени

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

9.1.5 Ограничения на имена

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего Центра являются:

Common Name (CN) - Фамилия, имя, отчество или псевдоним;

Organization (O) - Наименование организации, являющейся владельцем Удостоверяющего Центра;

Organization Unit (OU) - Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего Центра;

Email(E) - Адрес электронной почты;

Country(C) – RU;

State (S) - Субъект Федерации, где зарегистрирована организация, являющейся владельцем Удостоверяющего Центра.

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

Common Name (CN) - Фамилия, имя, отчество или псевдоним;

Email (E)- Адрес электронной почты;

Country (C) – RU;

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

Common Name (CN) - Фамилия, имя, отчество или псевдоним;

Organization (O) - Наименование организации, которую представляет владелец сертификата;

Email (E)- Адрес электронной почты;

Country (C) – RU;

State (S) – Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата.

9.2 Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме

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

9.2.1 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

10 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);

10.1 Программный комплекс обеспечения реализации целевых функций Удостоверяющего Центра

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

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

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

1. Формирования сертификатов ключей подписи 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 ключей подписи 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 ключей подписи пользователей УЦ;
3. Ведения эталонной копии Реестра сертификатов ключей подписи Удостоверяющего Центра;
4. Ведения эталонной копии списка аннулированных (отозванных) и приостановленных сертификатов ключей подписи 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 ключей подписи Удостоверяющего Центра;
3. Ведения Реестра заявлений на изготовление сертификатов ключей подписи пользователей УЦ в электронной форме;
4. Ведения Реестра заявлений на аннулирование (отзыв) сертификатов ключей подписи пользователей УЦ в электронной форме;

5. Ведения Реестра заявлений на приостановление действия сертификатов ключей подписи пользователей УЦ в электронной форме;
6. Ведения Реестра запросов на изготовление ключа подписи пользователей УЦ в электронной форме;
7. Ведения Реестра заявлений на возобновление действия сертификатов ключей подписи пользователей УЦ в электронной форме;
8. Предоставления программных средств для:
 - а. Пользователей УЦ Группы 1 для обеспечения реализации их права передать по сети на Удостоверяющий Центр запрос на изготовление ключа подписи в электронной форме;
 - б. Зарегистрированных пользователей УЦ Группы 2 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 УЦ.

АРМ разбора конфликтных ситуаций является приложением ПК УЦ и предназначен для 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.

10.2 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 Удостоверяющего Центра;
- Устройства печати на бумажных носителях (принтеры).

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

10.3 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.

10.4 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 изготовление ключа подписи;
- Принят запрос на изготовление ключа подписи;
- Отклонен запрос на изготовление ключа подписи;
- 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.

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

При эксплуатации программного комплекса обеспечения реализации целевых функций Удостоверяющего Центра ежедневно 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.

11 Обеспечение безопасности

11.1 Инженерно-технические меры защиты информации

11.1.1 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.

Остальные технические средства Удостоверяющего Центра размещаются в рабочих помещениях Удостоверяющего Центра по схеме организации рабочих мест персонала, утверждаемой Руководителем УЦ.

11.1.2 Физический доступ в помещения

Серверное помещение Удостоверяющего Центра оборудовано системой контроля доступа с идентификацией по проксимити карте. Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

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

Идентификационные карты для доступа в серверное помещение выдаются отделом технического обеспечения по согласованию со службой информационной безопасности, утверждение руководителя Удостоверяющего Центра.

Ключи магнитных замков рабочих помещений Удостоверяющего Центра выдаются сотрудникам на основании схемы организации рабочих мест персонала.

11.1.3 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 3 часов после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников Удостоверяющего Центра, подключены к источникам бесперебойного питания, обеспечивающие их работу в течение 30 минут после прекращения основного электроснабжения.

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.

11.1.4 Предупреждение и защита от возгорания

Серверное помещение Удостоверяющего Центра оборудовано системой пожарной сигнализации.

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

11.1.5 Хранение документированной информации

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

11.1.6 Уничтожение документированной информации

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

11.2 Программно-аппаратные меры защиты информации

11.2.1 Организация доступа к техническим средствам Удостоверяющего Центра

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

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

11.2.2 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» также оснащено 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 УЦ, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения (Центра Сертификации и/или Центра Регистрации).

Общий перечень объектов доступа УЦ

К объектам доступа Удостоверяющего центра относятся:

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

11.2.3 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;

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 – ежедневно.

11.2.4 Контроль целостности технических средств

Контроль целостности 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.

Перечень информации, подлежащей защите

Поступающая в Удостоверяющий Центр информация:

- Заявление на изготовление сертификата открытого ключа в электронной форме;
- Ключевая фраза пользователя УЦ.

Передаваемая из Удостоверяющего Центра информация:

- 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 ключей подписи пользователя УЦ и их статус.

11.3 Организационные меры защиты информации

11.3.1 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 5 лет. Сотрудники УЦ имеют высшее профессиональное образование или прошли курсы повышения квалификации в области информационной безопасности.

11.3.2 Профессиональная переподготовка и повышение квалификации персонала Удостоверяющего центра

Профессиональная переподготовка персонала Удостоверяющего Центра не осуществляется. Сотрудники Удостоверяющего Центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 5 лет.

11.3.3 Организация сменной работы Удостоверяющего центра

Деятельность Удостоверяющего Центра по работе с пользователями УЦ в части приема заявлений в бумажной форме и изготовления сертификатов ключей подписи организована в одну рабочую смену с 9.30 до 17.30 в будние дни. Выходными днями являются: суббота, воскресенье, а также дни общенациональных праздников.

11.3.4 Организация доступа персонала к документам и документации Удостоверяющего центра

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

11.4 Юридические меры защиты информации

Удостоверяющий Центр имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг Системы безопасности Удостоверяющего Центра и защиты информации созданы и поддерживаются владельцем УЦ самостоятельно, на основании лицензий, полученных в соответствии с действующим законодательством Российской Федерации.

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.

12 Взаимодействие 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 ключей подписи 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 распечатывает сертификат ключа подписи уполномоченного лица Удостоверяющего центра на бумажном носителе. Данный сертификат визируются собственноручной подписью уполномоченного лица Удостоверяющего центра, руководителя УЦ и заверяется печатью Удостоверяющего центра.

Ответственный сотрудник Удостоверяющего центра 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>.

13 Формирование объектных идентификаторов областей применения сертификатов открытых ключей

Регистрация частного номера ЗАО «Орбита» в российском сегменте мирового пространства идентификаторов осуществлена Уполномоченным федеральным органом исполнительной власти РФ по применению ЭЦП.

Удостоверяющий центр самостоятельно формирует объектные идентификаторы в соответствии с RFC 1098.

Список используемых объектных идентификаторов областей применения сертификатов открытых ключей представляет собой отдельный документ подписанный Руководителем УЦ.

Приложение 1.

Сокращения

CRL	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
ТМ	Устройство хранения информации на таблетке touch-memory
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПК	Программный комплекс
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина. Персональный компьютер
РИК	Российская интеллектуальная карта
СА	Системный администратор
СКЗИ	Средство криптографической защиты информации
СОС(crl)	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник.
ТЗ	Техническое задание
ЦС	Центр Сертификации
ЦР	Центр Регистрации
УЛ	Уполномоченное лицо
УФО	Уполномоченный федеральный орган
УЦ	Удостоверяющий Центр
ЭД	Электронный документ
ЭЗ	Электронный замок
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 ключа подписи - 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.