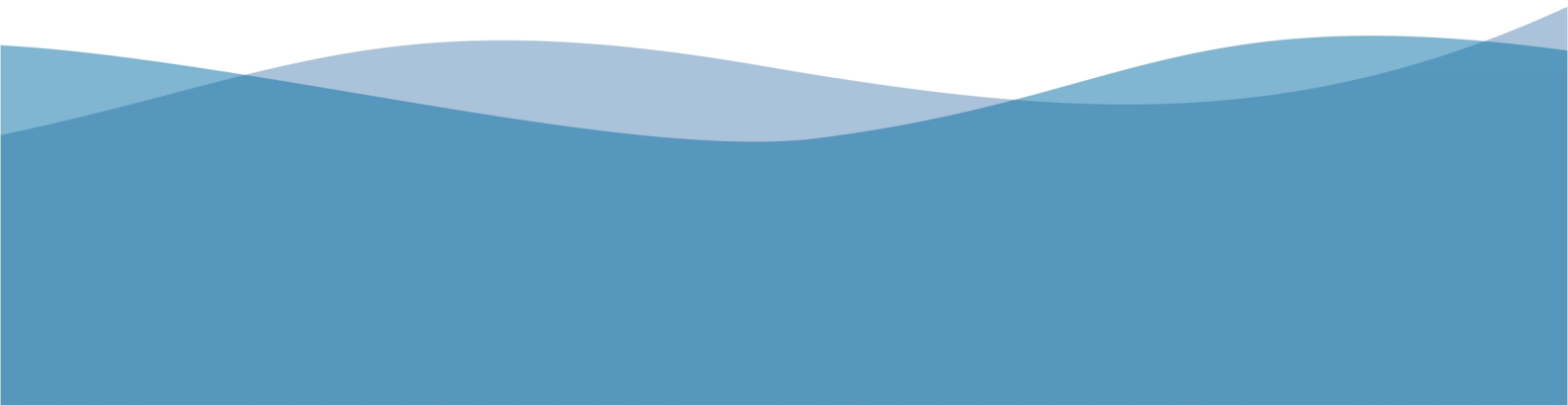


DTG

Регламент Удостоверяющего Центра

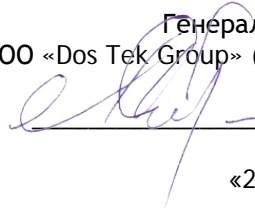




ОсОО «Dos Tek Group»
Кыргызская Республика
г. Бишкек, ул. Тыныстанова 189а

тел.: +996 312 909767
e-mail: office@dostek.kg
www.dostek.kg

УТВЕРЖДАЮ:
Генеральный директор
ОсОО «Dos Tek Group» (Дос Тек Групп)



Д. Мамбетов

«20» июня 2011 г.

Регламент Удостоверяющего Центра ОсОО «Dos Tek Group» (Дос Тек Групп)

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ	2
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
1. ОБЩИЕ ПОЛОЖЕНИЯ.....	6
1.1 ОБЗОРНАЯ ИНФОРМАЦИЯ.....	6
1.2 ОБЛАСТЬ ПРИМЕНЕНИЯ РЕГЛАМЕНТА	7
1.3 ПУБЛИКАЦИЯ РЕГЛАМЕНТА	7
1.4 СРОК ДЕЙСТВИЯ РЕГЛАМЕНТА И ПОРЯДОК ПРЕКРАЩЕНИЯ ЕГО ДЕЙСТВИЯ	7
1.5 ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ	8
2. УДОСТОВЕРЯЮЩИЙ ЦЕНТР И ПОЛЬЗОВАТЕЛИ УСЛУГ УЦ	8
2.1 СВЕДЕНИЯ И РЕКВИЗИТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	8
2.2. РЕЕСТР УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	9
Реестр УЦ - набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию:	9
2.3. НАЗНАЧЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	9
2.4. УСЛУГИ, ОКАЗЫВАЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ	9
2.5. ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	10
2.6. ПОЛЬЗОВАТЕЛИ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	10
2.7. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ	11
3. ПРАВА И ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ	11
3.1. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	11
3.2. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ УЦ	13
3.3. ОТВЕТСТВЕННОСТЬ	14
4. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ	14
5. ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ИЗГОТОВЛЕНИЯ И УПРАВЛЕНИЯ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПОДПИСЕЙ.....	15
5.1. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ УЦ, ЯВЛЯЮЩИМИСЯ РАБОТНИКАМИ ОсОО «Dos Tek Group» (Дос Тек Групп).....	15
5.2. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ УЦ.....	15
5.3. ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА И ПРЕДОСТАВЛЕНИЕ ЕГО ВЛАДЕЛЬЦУ.....	15
5.3.1. Изготовление сертификата открытого ключа	16
5.3.2. Аннулирование (отзыв) сертификата открытого ключа	16
5.3.3. Приостановление действия сертификата открытого ключа	16
5.3.4. Возобновление действия сертификата открытого ключа	17
5.3.5. Хранение сертификата открытого ключа пользователей	17
6. ПРОЦЕДУРА РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ	18
7. ПОЛОЖЕНИЯ ПО ИСПОЛЬЗОВАНИЮ ОТКРЫТЫХ И ЗАКРЫТЫХ КЛЮЧЕЙ	19
7.1. ИДЕНТИФИЦИРУЮЩИЕ ДАННЫЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	19
7.2. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	19
7.3. ТРЕБОВАНИЯ К СРЕДСТВАМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ПОЛЬЗОВАТЕЛЕЙ УЦ	20
7.4. СРОКИ ДЕЙСТВИЯ ЗАКРЫТЫХ КЛЮЧЕЙ И СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ПОЛЬЗОВАТЕЛЕЙ	20
7.5. НАЗНАЧЕНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА, МЕРЫ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ	20
7.6. АРХИВНОЕ ХРАНЕНИЕ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ	21
7.7. УПРАВЛЕНИЕ КЛЮЧАМИ	21
7.7.1. Плановая смена открытого и закрытого ключа УЦ	21
7.7.2. Внеплановая смена открытого и закрытого ключа УЦ	22
7.7.3. Плановая смена ключей Пользователя УЦ	22
7.7.4. Внеплановая смена ключей Пользователя Удостоверяющего Центра	22
8. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ	23
8.1. БАЗОВЫЕ ПОЛЯ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА	23
8.2. ПОДДЕРЖИВАЕМЫЕ ОБЪЕКТНЫЕ ИДЕНТИФИКАТОРЫ АЛГОРИТМОВ	23
8.3. ОБЯЗАТЕЛЬНЫЕ АТРИБУТЫ ПОЛЕЙ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ	24
8.4. БАЗОВЫЕ ПОЛЯ СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ	24
9. ПРОГРАММНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	



.....	25
9.1. ПРОГРАММНЫЙ КОМПЛЕКС РЕАЛИЗУЮЩИЙ ФУНКЦИИ УЦ	25
9.2. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	27
9.3. ПЕРЕЧЕНЬ СОБЫТИЙ, РЕГИСТРИРУЕМЫХ ПРОГРАММНЫМ КОМПЛЕКСОМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	27
10. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ	28
10.1. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	28
10.2. ПРОГРАММНО-АППАРАТНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	29
10.3. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	29
ПРИЛОЖЕНИЕ №1	31
ПРИЛОЖЕНИЕ №2	32
ПРИЛОЖЕНИЕ №2.1	33
ПРИЛОЖЕНИЕ №3	34
ПРИЛОЖЕНИЕ №4	35
ПРИЛОЖЕНИЕ №5	36
ПРИЛОЖЕНИЕ №6	37
ПРИЛОЖЕНИЕ №7	38
ПРИЛОЖЕНИЕ №8	39
ПРИЛОЖЕНИЕ №9	40
ПРИЛОЖЕНИЕ №10	41

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

УЦ	Удостоверяющий центр ОсОО «Dos Tek Group» (Дос Тек Групп)
ЭЦП	Электронная цифровая подпись
КР	Кыргызская Республика
СОС	Список отозванных сертификатов
КУЦ	Корневой Удостоверяющий центр
ПУЦ	Подчиненный Удостоверяющий центр
УКЦ	Удостоверяющий и Ключевой центр
ЦУС	Центр управления сетью
СУ	Сетевой узел
СКЗИ	Средство криптографической защиты информации
ViPNet	Торговая марка программного обеспечения компании ОАО «Инфотекс» г.Москва

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Владелец сертификата ключа подписи - физическое лицо, на имя которого Удостоверяющим Центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электронные документы).

Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

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

Запрос на отзыв сертификата - сообщение, содержащее необходимую информацию для отзыва сертификата.

Инфраструктура открытых ключей (англ. PKI - Public Key Infrastructure) - технология аутентификации с помощью открытых ключей. Это комплексная система, которая связывает открытые ключи с личностью пользователя посредством Удостоверяющего Центра.

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 контейнеров.

Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Копия сертификата ключа подписи - документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра.

Контейнер - место для хранения закрытого ключа.

Ключевой Центр (КЦ) - компонент удостоверяющего центра. Входит в программу ViPNet [Удостоверяющий и Ключевой Центр]. Предназначен для формирования пользовательской ключевой информации. Эта программа формирует ключевую информацию на основе информации, поступающей из ЦУС. Созданные программой КЦ ключи передаются пользователям, после чего при наличии соответствующего ПО ViPNet пользователи сети смогут безопасно обмениваться конфиденциальной информацией.

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Плановая смена ключей - смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром пользователю информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Список отозванных сертификатов (СОС) - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения их срока действия.

Средство электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи, подтверждение подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронных цифровых подписей.

Программный комплекс «Удостоверяющий центр ViPNet» - Программный комплекс, предназначенный для обслуживания следующих запросов: на издание сертификатов ЭЦП, на отзыв, приостановление и возобновления приостановленного действия сертификатов пользователей УЦ, сформированных на сетевых узлах сети ViPNet или в Центрах регистрации для внешних пользователей.

Центр регистрации - компонент программного комплекса «Удостоверяющий Центр ViPNet» предназначенный для регистрации внешних пользователей, создания ключей подписи и формирования запросов на издание, приостановление, отзыв и возобновление сертификата ключа подписи.

Центр сертификации - компонент программного комплекса «Удостоверяющий Центр ViPNet» выполняющий функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

Центр управления сетью (ЦУС) - компонент программного комплекса «Удостоверяющий Центр ViPNet», предназначенный для формирования и изменения структуры корпоративной сети.

Электронная цифровая подпись (электронная подпись, ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 ОБЗОРНАЯ ИНФОРМАЦИЯ

Настоящий Регламент Подчиненного удостоверяющего центра общества с ограниченной ответственностью «DOS TEK GROUP» (ДОС ТЕК ГРУПП) {Далее по тексту - УЦ}, являющегося структурным подразделением общества с ограниченной ответственностью «DOS TEK GROUP» (ДОС ТЕК ГРУПП) разработан в соответствии с законами Кыргызской Республики «Об информатизации», «Об электронном документе и электронной цифровой подписи», Национальной стратегии «Информационно-коммуникационные технологии для развития Кыргызской Республики», утвержденной Указом Президента Кыргызской Республики от 10 марта 2002 года N 54 и иными законодательными актами Кыргызской Республики, регламентирующими деятельность удостоверяющих центров.

Настоящий Регламент устанавливает общий порядок и условия предоставления УЦ пользователю Системы защищенного обмена электронными документами, услуг по изготовлению и выдаче сертификатов ключей электронной цифровой подписи и дополнительных услуг, связанных с управлением сертификатами ключей подписи и шифрования, включая обязанности пользователей, и членов группы администрирования УЦ, режимы работы, принятые форматы данных и мероприятия, необходимые для безопасной работы УЦ.

Целью настоящего Регламента является создание условий для организации взаимодействия информационных систем и правовых условий использования электронной цифровой подписи, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

Настоящий Регламент является договором присоединения в соответствии со статьей 387 Гражданского кодекса Кыргызской Республики. Присоединение к Регламенту производится путем заключения пользователем Системы защищенного обмена электронными документами соглашения о присоединении к Регламенту УЦ, указанного в Приложении № 1 к Регламенту. Факт присоединения к Регламенту является полным принятием Пользователем условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Соглашения о присоединении. После присоединения Пользователя к Регламенту, Стороны вступают в соответствующие договорные отношения на неопределенный срок.

1.2 ОБЛАСТЬ ПРИМЕНЕНИЯ РЕГЛАМЕНТА

Настоящий Регламент предназначен служить соглашением, налагающим обязательства на все вовлеченные Стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ. Регламент применим при организации защищенного обмена электронными документами и взаимодействия информационных систем.

1.3 ПУБЛИКАЦИЯ РЕГЛАМЕНТА

Настоящий Регламент распространяется:

в электронной форме:

- на информационном портале www.dostek.kg «DOS TEK GROUP» (ДОС ТЕК ГРУПП) в разделе «Удостоверяющий Центр», «Регламент удостоверяющего центра»;
- на носителе, предоставляемым Пользователем при его подключении к Системе защищенного электронного обмена документами.

На бумажном носителе:

- Через почтовый адрес: 720014, Кыргызская Республика г. Бишкек, ул. Тыныстанова 189 А.

Регламент, предназначенный для распространения в электронной форме, распространяется в виде файла формата PDF.

Любое заинтересованное лицо может ознакомиться с Регламентом, либо по запросу получить его копию в УЦ за плату, не превышающую расходов на ее изготовление. Справки по вопросам, связанным с оказанием услуг УЦ предоставляются по телефону +996 (312) 909-767.

1.4 СРОК ДЕЙСТВИЯ РЕГЛАМЕНТА И ПОРЯДОК ПРЕКРАЩЕНИЯ ЕГО ДЕЙСТВИЯ

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента устанавливается в пять лет.

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

Официальное уведомление о прекращении действия Регламента публикуется на информационном портале www.dostek.kg «DOS TEK GROUP» (ДОС ТЕК ГРУПП) в разделе «Удостоверяющий Центр», «Регламент удостоверяющего центра».

Взаимодействие Пользователя и УЦ в рамках настоящего Регламента может быть прекращено в случаях нарушения сторонами условий Регламента, либо по взаимному соглашению сторон. Инициативная сторона письменно уведомляет другую сторону о своих намерениях за тридцать календарных дней до даты прекращения взаимодействия Пользователя и УЦ. Данное Уведомление, является основанием для обязательного аннулирования сертификатов ключей подписей Пользователей УЦ, уполномоченных данным Пользователем. Датой аннулирования указанных сертификатов ключей Пользователей УЦ будет дата расторжения Соглашения.

Прекращение взаимоотношений Пользователя УЦ и Удостоверяющего Центра не освобождает Стороны от исполнения обязательств, возникших до указанного прекращения, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

1.5 ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

Внесение изменений (дополнений) в Регламент, в том числе Приложений к нему, производится УЦ в одностороннем порядке. Публикация изменений и дополнений осуществляется в порядке, соответствующему порядку утверждения и публикации Регламента. Все изменения и дополнения, вносимые в Регламент, и не связанные с изменением законодательства Кыргызской Республики вступают в силу и становятся обязательными для Сторон по истечении 10 (Десяти) календарных дней с даты размещения, указанных изменений и дополнений в Регламенте на информационном портале www.dostek.kg «DOS TEK GROUP» (ДОС ТЕК ГРУПП).

Все изменения и дополнения, вносимые в Регламент в связи с изменением законодательства Кыргызской Республики, вступают в силу одновременно с вступлением в силу изменений и дополнений в нормативных правовых актах.

Действие изменений и дополнений в Регламенте с момента их вступления в силу распространяется на всех Пользователей УЦ, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

2. УДОСТОВЕРЯЮЩИЙ ЦЕНТР И ПОЛЬЗОВАТЕЛИ УСЛУГ УЦ

2.1 СВЕДЕНИЯ И РЕКВИЗИТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Полное наименование Удостоверяющего центра: Удостоверяющий центр Общества с ограниченной ответственностью «DOS TEK GROUP» (ДОС ТЕК ГРУПП).

Местонахождение: г. Бишкек, ул. Тыныстанова 189 А

Юридический адрес ОсОО «DOS TEK GROUP» (ДОС ТЕК ГРУПП): 720014, Кыргызская Республика, г. Бишкек, ул. Суюмбаева 14 А

Банковские реквизиты: р/с 1280010015061112 ЗАО «Кыргызский Инвестиционный Кредитный Банк» БИК 128001

Зарегистрировано в УКГНС Октябрьского района ИНН 00211200910051

Регистрационный номер в Социальном фонде №04-58756 по Октябрьскому району ОРУСФ 6 мкр., д. 22/1

Руководитель: Генеральный директор - Мамбетов Дильмурат Турарович

Адрес электронной почты: pki@dostek.kg

Контактный телефон УЦ: +996(312) 909-767 Факс: +996(312) 664-774

УЦ в качестве участника предоставления услуг по изготовлению и выдаче сертификатов ключей подписи осуществляет свою деятельность на территории Кыргызской Республики на основании:

- Свидетельства о Государственной перерегистрации юридического лица серия ГПР



- №0090301, выданного Министерством юстиции Кыргызской Республики «10» марта 2010 г.;
- Сертификата Подчиненного Удостоверяющего Цента, выданного Государственным Предприятием «Инфоком» при Государственной Регистрационной Службе при Правительстве Кыргызской Республики со сроком действия с 22 июня 2010 года по 22 июня 2017 года
Серийный номер сертификата 61 02 d0 d3 00 00 00 00 0b

2.2. РЕЕСТР УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Реестр УЦ - набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр зарегистрированных пользователей УЦ;
- реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;
- реестр заявлений на приостановление/возобновление действия сертификата ключа подписи;
- реестр сертификатов ключей подписи;
- реестр списков отозванных сертификатов;
- служебные документы УЦ.

2.3. НАЗНАЧЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

УЦ предназначен для осуществления услуг в сфере инфраструктуры открытых ключей, обеспечивая участников информационного взаимодействия средствами и спецификациями для использования сертификатов ключей в целях обеспечения:

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

2.4. УСЛУГИ, ОКАЗЫВАЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

В процессе своей деятельности УЦ принимает на себя обязательство по оказанию Пользователям следующих видов услуг:

- внесение в реестр УЦ регистрационной информации о Пользователях;
- формирование закрытых и открытых ключей по обращениям пользователей УЦ, с записью их на ключевой носитель;
- ведение реестра изготовленных сертификатов открытых ключей пользователей УЦ;
- изготовление копии сертификатов открытых ключей пользователей УЦ на бумажном носителе;
- предоставление копий сертификатов открытых ключей в электронной форме, находящихся в реестре изготовленных сертификатов;
- аннулирование (отзыв) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
- приостановление и возобновление действия сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
- предоставление пользователям УЦ сведений об аннулированных и приостановленных



- сертификатах открытых ключей;
- подтверждение подлинности электронных цифровых подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ.

2.5. ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- обеспечение информационной безопасности и технической эксплуатации УЦ;
- управление деятельностью УЦ;
- взаимодействие с пользователями УЦ в части разрешения вопросов, связанных с применением средств ЭЦП, ключей и сертификатов открытых ключей, изготавливаемых и/или распространяемых УЦ;
- взаимодействие с пользователями УЦ в части разрешения вопросов, связанных с подтверждением электронной цифровой подписи в сертификатах открытых ключей, изготовленных УЦ;
- регистрация пользователей УЦ;
- ведение реестра зарегистрированных пользователей УЦ;
- распространение средств электронной цифровой подписи и шифрования;
- организация и выполнение мероприятий по защите ресурсов УЦ;
- формирование и обновление справочно-ключевой информации для организации защищенного обмена информации в рамках сети УЦ;
- изготовление и предоставление ключей по обращению пользователей УЦ;
- изготовление и предоставление изготовленных сертификатов открытых ключей в электронной форме по обращению пользователей УЦ;
- изготовление и предоставление копий сертификатов открытых ключей на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
- приостановление и возобновление действия сертификатов открытых ключей по обращению владельцев сертификатов открытых ключей;
- предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах открытых ключей;
- предоставление копий сертификатов открытых ключей, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
- техническое обеспечение процедуры подтверждения электронной цифровой подписи в документах, представленных в электронной форме, по обращениям пользователей УЦ.

2.6. ПОЛЬЗОВАТЕЛИ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Пользователи УЦ

Пользователями УЦ могут быть как физические лица, так и юридические лица, зарегистрированные в УЦ в соответствии с соглашением о присоединении к Регламенту.

Владельцы сертификатов

Владельцем сертификата может быть только физическое лицо.

В случае, когда в качестве Пользователя выступает юридическое лицо, то его интересы представляет физическое лицо (Уполномоченный Представитель) при наличии Доверенности (Приложение № 10), предоставляющей права данному физическому лицу представлять его интересы и наделяющей правом расписываться в соответствующих документах УЦ для исполнения поручений, определенных настоящей Доверенностью.

Пользователи сертификатов открытых ключей ЭЦП

Пользователями сертификатов (Доверенными участниками) могут быть любые лица, которым владельцы сертификатов доверяют использовать их сертификаты.

2.7. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ

УЦ осуществляет свою деятельность на платной основе. Стоимость работ и услуг определяется прейскурантом цен указанном на официальном портале УЦ www.dostek.kg на момент подписания «Соглашения о присоединении к Регламенту УЦ» (Приложение №1). Перечень и стоимость дополнительных услуг УЦ согласовывается в каждом конкретном случае.

По факту изготовления сертификатов ключей подписей УЦ выставляет Стороне, присоединившейся к Регламенту, счет на оплату изготовленных сертификатов ключей подписей. Сторона, присоединившаяся к Регламенту, обязуется оплатить счет в течение 5 (Пяти) банковских дней с момента его получения наличными денежными средствами, либо перечислением на расчетный счет УЦ.

Результат выполненных работ оформляется путем подписания «Сертификата ключа подписи» на бумажном носителе (Приложение № 10) между пользователем и УЦ.

3. ПРАВА И ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ

3.1. ПРАВ А И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

УЦ обязан:

- Использовать для изготовления закрытых ключей и формирования электронной цифровой подписи, только средства криптографической защиты информации, в соответствии с действующим законодательством Кыргызской Республики;
- Использовать закрытый ключ УЦ только для подписи издаваемых им сертификатов открытых ключей и списков отозванных сертификатов;
- Принять меры по защите закрытого ключа УЦ в соответствии с положениями настоящего Регламента;
- Синхронизировать по времени все программные и технические средства по GMT (Greenwich Mean Time) с учетом часового пояса;
- Обеспечить регистрацию пользователей УЦ по заявлениям на регистрацию, в соответствии, с порядком регистрации, изложенным в настоящем Регламенте;
- Обеспечить уникальность регистрационной информации пользователей УЦ, заносимой в реестр УЦ;
- Не разглашать (публиковать) регистрационную информацию пользователей УЦ, за исключением информации используемой для идентификации владельцев сертификатов открытых ключей и заносимой в изготавливаемые сертификаты. Публикация информации, используемой для идентификации владельцев сертификатов открытых ключей, осуществляется путем включения ее в изготавливаемые сертификаты;
- Изготовить закрытый и открытый ключ пользователю по заявлению с использованием средства

- криптографической защиты информации, в соответствии с действующим законодательством Кыргызской Республики;
- Выполнять процедуру генерации ключей и запись ключей на отчуждаемый носитель;
 - Обеспечить изготовление сертификата открытого ключа пользователю по заявлению, в соответствии с форматом и порядком идентификации владельца сертификата открытого ключа, определенным в настоящем Регламенте;
 - Обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов открытых ключей пользователей УЦ;
 - Обеспечить уникальность значений открытых ключей в изготовленных сертификатах открытых ключей пользователей УЦ;
 - УЦ обеспечивает изготовление двух копий сертификата ключа подписи на бумажном носителе по форме, определенной Приложением №10 настоящего Регламента. Все копии сертификата ключа подписи на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру регистрации, или собственноручной подписью его доверенного представителя, а также собственноручной подписью уполномоченного лица УЦ ответственного за регистрацию;
 - Аннулировать (отозвать) сертификат открытого ключа по заявлению его владельца;
 - В течение одного рабочего дня занести сведения об аннулированном (отозванном) сертификате в список отозванных сертификатов с указанием даты и времени занесения;
 - Приостановить действие сертификата открытого ключа по заявлению его владельца;
 - В течение одного рабочего дня занести сведения о приостановленном сертификате в список отозванных сертификатов с указанием даты и времени занесения и признака приостановления;
 - Возобновить действие сертификата открытого ключа по заявлению его владельца (если было приостановлено действие сертификата);
 - В течение одного рабочего дня исключить сведения о приостановленном сертификате из списка отозванных сертификатов;
 - Уведомить о факте изготовления сертификата открытого ключа его владельца. Срок уведомления - не позднее двух рабочих дней с момента изготовления сертификата открытого ключа;
 - Официально уведомить о факте аннулирования (отзыва), приостановлении и возобновлении действия сертификата ключа подписи лиц, зарегистрированных в УЦ. Срок уведомления - не позднее одного рабочего дня с момента занесения сведений об аннулированном (отозванном), приостановленном, возобновленном сертификате в список отозванных сертификатов. Официальным уведомлением является публикация списка отозванных сертификатов на информационном портале www.dostek.kg в разделе «Удостоверяющий Центр», «Список Отозванных Сертификатов» Временем аннулирования (отзыва), приостановления, возобновления сертификата ключа признается время занесения сведений в список отозванных сертификатов и включенное в его структуру;
 - Осуществлять выдачу копий сертификатов открытых ключей в электронной форме по обращениям пользователей УЦ;
 - Уведомлять владельца сертификата открытого ключа о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата открытого ключа.

УЦ имеет право:

- Предоставлять копии сертификатов открытых ключей в электронной форме, находящихся в реестре УЦ, всем Пользователям УЦ, обратившимся за копиями в УЦ;
- Отказать в изготовлении сертификата открытого ключа зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата открытого ключа, с указанием причин отказа;
- Аннулировать (отозвать) сертификат открытого ключа пользователя УЦ в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением владельца аннулированного (отозванного) сертификата открытого ключа;
- В одностороннем порядке приостановить или отозвать действие сертификата открытого ключа

пользователя УЦ, с обязательным уведомлением владельца приостановленного сертификата открытого ключа и указанием обоснованных причин:

1. своевременная неуплата за услуги УЦ;
2. по распоряжению уполномоченных Государственных органов;
3. нарушения пунктов настоящего Регламента.

3.2. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ УЦ

Обязанности пользователей УЦ:

- лица, проходящие процедуру регистрации в реестре УЦ, обязаны предоставить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента;
- хранить в тайне закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
- использовать закрытый ключ только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;
- немедленно обратиться в УЦ с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также, в случае если пользователю УЦ стало известно, что этот ключ используется или использовался ранее другими лицами;
- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата в УЦ по момент времени официального уведомления об аннулировании (отзыве) сертификата, либо об отказе в аннулировании (отзыве);
- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в УЦ по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия;
- не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован (отозван) или действие его приостановлено;
- перед тем как использовать сертификат открытого ключа, изготовленный УЦ, пользователь сертификата должен удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту, соответствует предполагаемому использованию.
- провести согласование с УЦ использование неописанных в Регламенте областей применения сертификата открытого ключа.

Пользователи УЦ имеют права:

- обратиться в УЦ для изготовления закрытых и открытых ключей с записью их на ключевой носитель;
- получить и ввести в действие на своем рабочем месте изготовленный сертификат открытого ключа в электронной форме;

- обратиться в УЦ для внесения в реестр УЦ регистрационной информации о пользователе УЦ, с целью в дальнейшем стать владельцем сертификата открытого ключа;
- получить список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный УЦ;
- получить сертификат открытого ключа УЦ;
- применять сертификат открытого ключа УЦ для проверки электронной цифровой подписи УЦ в сертификатах открытого ключа, изготовленных УЦ.
- применять список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный УЦ, для проверки статуса сертификатов открытых ключей подписи;
- обратиться в УЦ за подтверждением подлинности электронных цифровых подписей УЦ в изготовленных им сертификатах открытых ключей;
- обратиться в УЦ по истечению срока действия сертификата открытого ключа; для изготовления нового сертификата открытого ключа.

3.3. ОТВЕТСТВЕННОСТЬ

В случае невыполнения Стороной, присоединившейся к Регламенту, обязательств по оплате изготовленных сертификатов ключей подписей, изложенных в разделе 2.7. настоящего Регламента, УЦ имеет право приостановить действие изготовленных сертификатов ключей подписей.

За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за не полученные доходы (упущенную выгоду), которые бы получила другая Сторона

Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств

Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Кыргызской Республики.

4. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

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

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

Информация, не являющаяся конфиденциальной, публикуется по решению УЦ. Место, способ и время публикации определяется решением УЦ.

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

Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной



Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях установленных законодательством Кыргызской Республики.

5. ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ИЗГОТОВЛЕНИЯ И УПРАВЛЕНИЯ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПОДПИСЕЙ

Процедура регистрации пользователей УЦ применяется в отношении лиц, присоединившихся к Регламенту, обращающихся за услугами в УЦ в части изготовления сертификатов открытых и закрытых ключей пользователей УЦ с записью их на ключевой носитель и предоставившие перечень необходимых документов и приложений:

- Соглашение о присоединении к регламенту (Приложение №1);
- Доверенность на получение и использование ключей ЭЦП (если необходимо) (Приложение №2);
- Соответствующее заявление на изготовление сертификата ключа подписи (для физического лица или юридического лица или органы государственной власти и управления) (Приложения №3, №4, №5);
- Сертификат ключа подписи (Приложение №10);
- Копия паспорта;
- Копия свидетельства о регистрации/перерегистрации (для юридических лиц и органов государственной власти и управления).

Изготовление ключей выполняется оператором УЦ на специализированном рабочем месте, в соответствии с принятым заявлением. Изготовленные ключи записываются на ключевой носитель

5.1. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ УЦ, ЯВЛЯЮЩИМИСЯ РАБОТНИКАМИ ОсОО «Dos Tek Group» (Дос Тек Групп)

Регистрация пользователей УЦ, являющихся работниками ОсОО «Dos Tek Group» (Дос Тек Групп), осуществляется на основании заявок руководителей отделов.

5.2. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ УЦ

Идентификация пользователя УЦ осуществляется по информации, занесенной в реестр УЦ.

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

Аутентификация пользователя УЦ по сертификату открытого ключа выполняется путем выполнения процедуры подтверждения электронной цифровой подписи с использованием сертификата открытого ключа.

5.3. ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА И ПРЕДОСТАВЛЕНИЕ ЕГО ВЛАДЕЛЬЦУ

5.3.1. Изготовление сертификата открытого ключа

Изготовление сертификата открытого ключа осуществляется оператором УЦ на основании заявления на изготовление сертификата открытого ключа. Срок рассмотрения заявления на изготовление сертификата открытого ключа составляет два рабочих дня, с момента его поступления. Изготовленный сертификат открытого ключа в электронной форме, заверенный электронной цифровой подписью УЦ, предоставляется его владельцу при личном обращении в УЦ. Также предоставляется копия сертификата открытого ключа на бумажном носителе

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

Заявление включает в себя следующие обязательные реквизиты:

- Фамилию, имя, отчество заявителя;
- Дата и подпись заявителя;
- Текст запроса на сертификат.

Владелец сертификата открытого ключа идентифицируется по значениям атрибутов поля Subject (Субъект) сертификата открытого ключа (см. раздел [8.3.] настоящего Регламента).

5.3.2. Аннулирование (отзыв) сертификата открытого ключа

Аннулирование (отзыв) сертификата открытого ключа изготовленного УЦ, осуществляется УЦ по заявлению на отзыв сертификата открытого ключа его владельца (Приложение №6).

Заявление на отзыв сертификата открытого ключа в бумажной форме подается заявителем в УЦ лично. Срок рассмотрения заявления на отзыв сертификата открытого ключа составляет один рабочий день с момента его поступления в УЦ.

Официальным уведомлением о прекращении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено.

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.

5.3.3. Приостановление действия сертификата открытого ключа

Приостановление действия сертификата открытого ключа изготовленного УЦ, осуществляется УЦ по заявлению на приостановление действия сертификата открытого ключа его владельца (Приложение №7).



Заявление на приостановление действия сертификата открытого ключа в бумажной форме подается заявителем в УЦ лично. Срок рассмотрения заявления на приостановление действия сертификата открытого ключа составляет один рабочий день с момента его поступления в УЦ.

Официальным уведомлением о приостановлении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено.

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.

5.3.4. Возобновление действия сертификата открытого ключа.

Возобновление действия сертификата открытого ключа изготовленного УЦ, осуществляется УЦ по заявлению на возобновление действия сертификата открытого ключа его владельца (Приложение №8).

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 два рабочих дня с момента его поступления в УЦ.

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.

5.3.5. Хранение сертификата открытого ключа пользователей

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

Срок архивного хранения сертификата открытого ключа устанавливается в соответствии со сроком, определенным разделом [7.6] настоящего Регламента.

6. ПРОЦЕДУРА РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ

В период использования сертификатов открытых ключей, изданных УЦ, могут возникать конфликтные ситуации с контейнером, открытым и/или закрытым ключом подписи пользователя, связанные с непризнанием ими целостности, подлинности или авторства, а также статуса электронной цифровой подписи.

В случае возникновения конфликтной ситуации пользователь, предполагающий возникновение конфликтной ситуации, должен направить в отдел УЦ уведомление о конфликтной ситуации с изложением обстоятельств ее возникновения и в каждом конкретном случае дополнительную информацию, которая потребуется для решения конфликтной ситуации.

УЦ проверяет наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направляет пользователю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если пользователь удовлетворен информацией, полученной от УЦ.

В случае если пользователь не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза.

В случае невозможности разрешения конфликтной ситуации в рабочем порядке и по итогам работы технической экспертизы, конфликтная ситуация рассматривается в судебном порядке, согласно действующему законодательству Кыргызской Республики.

Экспертная комиссия создается УЦ на основании письменного заявления (претензии) Стороны пользователя. В указанном заявлении должно быть указано лицо (лица), уполномоченные представлять интересы Стороны в составе экспертной комиссии, количество указанных лиц не может превышать 3 (Три) человека.

Не позднее 10 (Десяти) рабочих дней с момента получения претензии назначается дата, место и время начала работы комиссии, о чем уведомляются обе Стороны по телефону, факсу или электронной почте.

Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. В случае, если представители одной из Сторон не явились для участия в экспертной комиссии, экспертиза проводится без их участия, а об отсутствии представителей составляется акт, подписываемый всеми присутствующими участниками экспертной комиссии.

Экспертиза осуществляется на предоставленном Удостоверяющим Центром персональном компьютере с установленным ПО ViPNet.

Экспертиза осуществляется в два этапа:

- Проверка оборудования и программного обеспечения и тестирование их работоспособности;
- Проверка целостности, принадлежности и актуальности: контейнера, открытого и закрытого ключа подписи пользователя



Проверка работоспособности и контроль целостности сертификата ключа подписи производится пробной подписью и проверкой в присутствии членов экспертной комиссии.

Проверка принадлежности, актуальности и целостности сертификата ключей подписи производится путем вызова в программе диалога просмотра сертификата, распечатывания на бумажном носителе и сравнения членами экспертной комиссии с соответствующим сертификатом из реестра УЦ. Члены комиссии производят визуальную сверку данных сертификатов.

Результаты экспертизы оформляются в виде письменного заключения - Акта экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения экспертизы. В Акте фиксируются результаты всех этапов проведенной экспертизы. Акт составляется по одному экземпляру для каждой из Сторон. Акт комиссии является окончательным и пересмотру не подлежит.

В случае невозможности разрешения конфликтной ситуации в рабочем порядке и по итогам работы технической экспертизы, конфликтная ситуация рассматривается в судебном порядке, согласно действующему законодательству Кыргызской Республики.

7. ПОЛОЖЕНИЯ ПО ИСПОЛЬЗОВАНИЮ ОТКРЫТЫХ И ЗАКРЫТЫХ КЛЮЧЕЙ

7.1. ИДЕНТИФИЦИРУЮЩИЕ ДАННЫЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Common Name (CN)	Общее имя	ПУЦ DOS TEK GROUP (ДОС ТЕК ГРУПП)
Organization Unit (OU)	Наименование подразделения	Подчиненный Удостоверяющий Центр DOS TEK GROUP (ДОС ТЕК ГРУПП)
Organization (O)	Организация	DOS TEK GROUP (ДОС ТЕК ГРУПП)
Location (L)	Локализация	Бишкек
Country (C)	Страна	KG
Email (E)	Электронная почта	pki@dostek.kg

7.2. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Срок действия закрытого ключа и открытого ключа, соответствующего закрытому ключу, УЦ составляет 7 (Семь) лет.

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

7.3. ТРЕБОВАНИЯ К СРЕДСТВАМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ПОЛЬЗОВАТЕЛЕЙ УЦ

Средство электронной цифровой подписи должно обеспечивать выполнение следующих процедур:

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

Средство электронной цифровой подписи должно обеспечивать выполнение мер защиты закрытых ключей.

В качестве средства электронной цифровой подписи пользователи должны использовать сертифицированные в соответствии с правилами сертификации средства криптографической защиты информации.

Идентификаторы алгоритмов представлены в настоящем Регламенте в разделе [8.2.].

7.4. СРОКИ ДЕЙСТВИЯ ЗАКРЫТЫХ КЛЮЧЕЙ И СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ПОЛЬЗОВАТЕЛЕЙ

Срок действия закрытого ключа пользователя УЦ, соответствующего сертификату открытого ключа, владельцем которого он является, составляет 12 (Двенадцать) месяцев.

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 действия сертификатов открытых ключей пользователей УЦ, составляет 1 (Один) год.

Срок действия сертификата открытого ключа устанавливается УЦ в момент его изготовления.

7.5. НАЗНАЧЕНИЕ КЛЮЧЕЙ И СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА, МЕРЫ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ

Ключи и сертификат открытого ключа предназначены для:

- обеспечения аутентификации и авторизации пользователя УЦ;
- формирования электронной цифровой подписи;
- использования в соответствии со сведениями, указанными в сертификате в областях использования.

Закрытые ключи пользователей УЦ должны записываться при их генерации на отчуждаемые носители ключевой информации.

Закрытые ключи на носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) рекомендуется формировать в согласии со следующими требованиями:

- Длина пароля (ПИН-кода) не меньше 6 символов;
- Пароль (ПИН-код) содержит символы цифр, буквы латинского алфавита, заглавные символы и спецсимволы.

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 УЦ, являющиеся владельцами закрытых ключей, также выполняют указанные в разделе меры защиты закрытых ключей.

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 Der или Base64.

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;
- Сведения об открытом ключе владельца сертификата и алгоритме его формирования;
- Сведения об областях использования закрытого ключа и сертификата;
- Собственноручную подпись оператора УЦ;
- Печать УЦ.

Копия сертификата открытого ключа печатается на листах белой бумаги формата А4.

7.6. АРХИВНОЕ ХРАНЕНИЕ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

Архивированию подлежит следующая документированная информация:

- Реестр сертификатов открытых ключей пользователей УЦ;
- Сертификаты открытых ключей УЦ;
- Реестр зарегистрированных пользователей УЦ;
- Заявления на изготовление ключей пользователей УЦ;
- Заявления на аннулирование (отзыв) сертификатов открытых ключей;
- Заявления на приостановление действия сертификатов открытых ключей;
- Заявления на возобновление действия сертификатов открытых ключей;
- Служебные документы УЦ.

Срок хранения архивных документов устанавливается 5 (Пять) лет.

7.7. УПРАВЛЕНИЕ КЛЮЧАМИ

7.7.1. Плановая смена открытого и закрытого ключа УЦ

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) УЦ выполняется в соответствии со сроком действия сертификата УЦ и осуществляется в следующем порядке:

- УЦ формирует запрос в Корневой Удостоверяющий Центр на создание нового сертификата открытого ключа УЦ;



- Корневой Удостоверяющий Центр обрабатывает запрос и формирует новый сертификат открытого ключа УЦ;
- УЦ вводит новый сертификат открытого ключа УЦ в эксплуатацию.

7.7.2. Внеплановая смена открытого и закрытого ключа УЦ

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа УЦ. При компрометации ключей УЦ прекращается работа по их использованию.

Процедура внеплановой смены ключей УЦ выполняется в следующем порядке:

- УЦ составляется заявление на аннулирование (отзыв) сертификата ключа подписи Удостоверяющего Центра и направляет его в Корневой Удостоверяющий Центр;
- Корневой Удостоверяющий Центр заносит в список отозванных сертификатов скомпрометированный сертификат открытого ключа УЦ;
- УЦ формирует запрос на новый сертификат открытого ключа УЦ в Корневой Удостоверяющий Центр;
- Корневой Удостоверяющий Центр выпускает новый сертификат открытого ключа УЦ;
- УЦ вводит новый сертификат открытого ключа УЦ в эксплуатацию.

7.7.3. Плановая смена ключей Пользователя УЦ

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Пользователя УЦ выполняется в соответствии со сроком действия сертификата Пользователя УЦ.

Процедура плановой смены ключей Пользователя УЦ осуществляется в следующем порядке:

- УЦ формирует новый закрытый и соответствующий ему открытый ключ;
- УЦ изготавливает сертификат нового открытого ключа пользователя УЦ и подписывает его электронной цифровой подписью

7.7.4. Внеплановая смена ключей Пользователя Удостоверяющего Центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа Пользователя УЦ. В случае компрометации ключей подписи Пользователь обязан немедленно сообщить об этом УЦ и не использовать эти ключи для формирования подписи.

Ключи пользователя могут считаться скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным отчуждаемый носитель с ключевой информацией;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере;
- уволился пользователь, имевший доступ к паролям и ключам.

Процедура внеплановой смены ключей выполняется в следующем порядке:

- УЦ аннулирует (отзывает) сертификаты открытых ключей пользователей путем занесения в список отозванных сертификатов;
- УЦ производит публикацию списка отозванных сертификатов;
- УЦ по запросу формирует новый сертификат открытого ключа пользователя УЦ.

8. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

Удостоверяющий Центр издает сертификаты открытых ключей пользователей УЦ в электронной форме формата X.509 версии 3, а списки отозванных сертификатов формата X.509 версии 2.

8.1. БАЗОВЫЕ ПОЛЯ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА

Сертификаты открытых ключей содержат следующие базовые поля X.509:

Серийный номер	Серийный номер сертификата открытого ключа
Алгоритм подписи	Используемый алгоритм для формирования ЭЦП
Поставщик	Идентифицирующие данные Удостоверяющего Центра
Действителен с ... по	Даты начала и окончания срока действия сертификата
Субъект	Идентифицирующие данные владельца сертификата открытого ключа
Открытый ключ	Значение открытого ключа алгоритма средства электронной цифровой подписи, с которыми используется данный открытый ключ.
Использования ключа	Область применения сертификата открытого ключа
Версия	Версия сертификата формата X.509

8.2. ПОДДЕРЖИВАЕМЫЕ ОБЪЕКТНЫЕ ИДЕНТИФИКАТОРЫ АЛГОРИТМОВ

ГОСТ Р 34.10-94	1.2.643.2.2.20	Алгоритм формирования открытых ключей
ГОСТ Р 34.10-2001	1.2.643.2.2.19	Алгоритм формирования открытых ключей
ГОСТ Р 34.10-94	1.2.643.2.2.4	Алгоритм подписи
Диффи-Хеллмана	1.2.643.2.2.99	Алгоритм на базе экспоненциальной функции
Диффи-Хеллмана	1.2.643.2.2.98	Алгоритм на базе эллиптической кривой
ГОСТ Р 34.11-94	1.2.643.2.2.9	Алгоритм функции хеширования
ГОСТ 28147-89	1.2.643.2.2.21	Алгоритм шифрования

8.3 .ОБЯЗАТЕЛЬНЫЕ АТТРИБУТЫ ПОЛЕЙ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ

В сертификате открытого ключа поля идентификационных данных владельца сертификата содержат атрибуты имени формата X.509.

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

Common Name (CN)	Общее Имя	Фамилия Имя Отчество физического лица
SerialNumber	Идентификационный номер	ИНН физического лица
Location (L)	Локализация	Место прописки физического лица
Country (C)	Страна	Страна
Email (E)	Электронная почта	Электронная почта физического лица

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

Common Name (CN)	Общее Имя	Фамилия Имя Отчество юридического лица
SerialNumber	Идентификационный номер	ИНН юридического лица
Organization (O)	Организация	Наименование организации
Location (L)	Локализация	Место регистрации юридического лица
Country (C)	Страна	Страна
Email (E)	Электронная почта	Электронная почта юридического лица

8.4. БАЗОВЫЕ ПОЛЯ СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ

Список отозванных сертификатов содержит следующие базовые поля X.509:

Поставщик	Идентифицирующие данные УЦ выпустившего СОС
Алгоритм подписи	Используемый алгоритм для формирования ЭЦП
Действителен с	Даты начала действия СОС
Следующее обновление	Даты следующего обновления СОС
Субъект	Идентифицирующие данные владельца сертификата открытого ключа



Версия	Версия СОС формата X.509
--------	--------------------------

УЦ использует следующие атрибуты СОС:

Серийный номер	Серийный номер сертификата открытого ключа
Дата отзыва	Дата и точное время отзыва
Код причины списка отзыва (CRL)	Код причины отзыва СОС

9. ПРОГРАММНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для реализации своих услуг УЦ используются следующие программные и технические средства:

- Программный комплекс «Удостоверяющий центр ViPNet» реализующий функции УЦ;
- Технические средства обеспечения работы программного комплекса УЦ;
- Программные и программно-аппаратные средства защиты информации.

Для обеспечения резервного восстановления программного комплекса УЦ, создаются архивные копии, которые формируются и хранятся согласно внутренним инструкциям УЦ.

9.1. ПРОГРАММНЫЙ КОМПЛЕКС РЕАЛИЗУЮЩИЙ ФУНКЦИИ УЦ

Программный комплекс «Удостоверяющий центр ViPNet» включает в себя следующие программные компоненты:

- Администратор
 - ViPNet [Администратор] [Центр управления сетью].
 - ViPNet [Администратор] [Удостоверяющий и ключевой центр].
 - ViPNet [Клиент] [Монитор]
 - ViPNet [Клиент] [Деловая почта]

ViPNet [Администратор] является базовым компонентом программного комплекса «Удостоверяющий центр ViPNet», включает в себя программы ViPNet [Администратор] [Центр управления сетью] и ViPNet [Удостоверяющий и Ключевой Центр].

Программа ViPNet [Администратор] [Центр управления сетью], далее ЦУС, предназначена для формирования и изменения структуры сети УЦ, и обеспечивает реализацию следующих целевых функций УЦ:

- Регистрация сетевых узлов (СУ);
- Распределение задач для СУ (Координатор, Клиент, Пункт регистрации);
- Регистрация клиентов (абонентов) в сети УЦ на СУ;



- Создание и изменение разрешенных связей для СУ;
- Формирование и рассылка адресных справочников для СУ;
- Формирование справочников для Удостоверяющего и ключевого центра (УКЦ);
- Рассылка для СУ обновлений справочно-ключевой информации, формируемой УКЦ;
- Рассылка для СУ списков отозванных сертификатов и списков сертификатов удостоверяющих центров;
- прием и передача в УКЦ запросов на сертификаты ключей подписи и обновление сертификатов от пользователей сети УЦ и Центров регистрации, рассылка изданных сертификатов на СУ.

Программа ViPNet [Удостоверяющий и Ключевой Центр] по функциям разделяется на две программы: Ключевой Центр и Удостоверяющий Центр.

Программа Ключевой Центр (КЦ) предназначена для формирования пользовательской ключевой информации. Эта программа формирует ключевую информацию на основе информации, поступающей из ЦУС. Созданные программой КЦ ключи передаются пользователям, после чего при наличии соответствующего ПО ViPNet пользователи сети УЦ смогут безопасно обмениваться конфиденциальной информацией.

КЦ обеспечивает реализацию следующих функций Удостоверяющего Центра:

- Формирование ключевых дискет для пользователей сети УЦ;
- Формирование ключевых наборов для сетевых узлов;
- Формирование паролей;
- Обновление ключевых дискет и ключевых наборов.

Программный комплекс «Удостоверяющий центр ViPNet» предназначен для обслуживания следующих запросов: на издание сертификатов ЭЦП, на отзыв, приостановление и возобновления приостановленного действия сертификатов пользователей УЦ, сформированных на сетевых узлах сети УЦ.

Программный комплекс «Удостоверяющий центр ViPNet» обеспечивает реализацию следующих функций УЦ:

- Создание ключей подписи и издание сертификатов УЦ;
- Регистрацию персональных данных внешнего пользователя.
- Ведение Реестра зарегистрированных внешних пользователей УЦ.
- Генерацию секретного ключа подписи и сохранение его на персональном ключевом носителе внешнего пользователя.
- Отправка запроса в Центр сертификации, прием и ввод в действие изданных сертификатов.
- Ведение Реестра справочников запросов и изданных сертификатов.
- Формирование запросов на отзыв, приостановление или возобновление сертификатов.
- Формирование запросов в КУЦ на издание сертификата УЦ;
- Создание ключей подписи пользователей и издание сертификатов сети УЦ по запросам ЦУС;
- Рассмотрение запросов на издание сертификатов ключей подписи от пользователей УЦ;
- Рассмотрение запросов от Центров регистрации на издание сертификатов ключей подписи внешних пользователей;
- Хранение информации о запросах и ведение Реестра справочников изданных сертификатов;

- Рассмотрение запросов на отзыв, приостановление и возобновление сертификатов;
- Отправка в ЦУС для обновления списков отозванных сертификатов;
- Ведение списка аннулированных (отозванных) и приостановленных сертификатов открытых ключей пользователей УЦ.

Программный комплекс «Удостоверяющий центр ViPNet» обеспечивает возможность формирования и сертификации ключей подписи для алгоритмов ГОСТ Р 34/10-94 и ГОСТ Р 34/10-2001.

9.2. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

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

- Средства криптографической защиты информации ViPNet;
- ViPNet [Координатор], предназначенный для обеспечения защищенного служебного информационного обмена между компонентами УЦ через открытые сети, реализующий все серверные функции в рамках сети ViPNet: сервер IP-адресов, межсетевой экран, сервер маршрутизатор и др.
- ViPNet [Клиент], обеспечивающий защиту компьютеров от несанкционированного доступа к различным информационным и аппаратным ресурсам на нем при работе компьютера в локальных или глобальных сетях.
- Устройства обеспечения бесперебойного питания серверов УЦ;
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений УЦ;
- Устройства обеспечения противопожарной безопасности помещений УЦ.

9.3. ПЕРЕЧЕНЬ СОБЫТИЙ, РЕГИСТРИРУЕМЫХ ПРОГРАММНЫМ КОМПЛЕКСОМ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- Вход администратора в программу УКЦ.
- Регистрация администратора УКЦ.
- Издание сертификата администратора УКЦ.
- Издание СОС.
- Принят запрос на сертификат открытого ключа.
- Отклонен запрос на издание открытого ключа.
- Издание сертификата открытого ключа.
- Принят запрос на отзыв сертификата.
- Удовлетворен запрос на отзыв сертификата.
- Отклонен запрос на отзыв сертификата.
- Системные события общесистемного программного обеспечения.

10. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

10.1. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Размещение технических средств УЦ

Серверы, сетевое и телекоммуникационное оборудование, системы хранения данных и вспомогательное оборудование размещены в выделенном Серверном помещении (далее по тексту - Серверная).

Остальные технические средства, рабочие станции УЦ размещены в рабочих помещениях УЦ по схеме организации рабочих мест сотрудников.

Физический доступ

Для Серверной устанавливается статус помещения ограниченного доступа с ограничением физического доступа посетителей.

Санкционированный доступ в Серверную происходит в соответствии со Списком доступа в серверное помещение. Порядок доступа в серверное помещение и Список доступа утверждается руководителем УЦ.

Серверное помещение УЦ оборудовано системой контроля доступа, охранной сигнализацией, видео наблюдением и системой пожаротушения

Электроснабжение и кондиционирование воздуха

Технические средства УЦ подключены к общегородской сети электроснабжения.

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

Серверы, сетевое и телекоммуникационное оборудование, системы хранения данных и вспомогательное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу при кратковременном отключении электропитания в течение 30 (Тридцать) минут и корректное завершение работы всех систем при более длительном отключении основного электроснабжения.

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

Подверженность воздействию влаги

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

Предупреждение и защита от возгорания

Серверное помещение УЦ оборудовано системой пожарной сигнализации.



Пожарная безопасность помещений УЦ обеспечивается в соответствии с нормами и требованиями противопожарной безопасности.

10.2. ПРОГРАММНО-АППАРАТНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Доступ к техническим средствам УЦ, размещенным в серверном помещении, разрешен только лицам из Списка доступа с использованием контроля доступа.

Ключи для доступа в серверное помещение сотрудникам выдает лицо ответственное за снятие и установку режима охраны Серверной.

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

Серверы оснащены программными комплексами защиты от несанкционированного доступа, имеющие сертификаты ФСТЭК.

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

- Программные модули средств электронной цифровой подписи и криптографической защиты информации;
- Программные модули программного обеспечения ViPNet Администратор;

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

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

Защита конфиденциальной информации, передаваемой между программно-техническими средствами сети УЦ, осуществляется путем шифрования информации с использованием сертифицированных криптографических средств защиты информации.

Перечень конфиденциальной информации, передаваемой из УЦ:

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

10.3. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Охрану здания и помещений выполняет служба безопасности, обеспечивающая:



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

Руководитель и инженерно-технические работники УЦ являются квалифицированными специалистами, к которым предъявляются следующие требования:

- Руководитель УЦ имеет высшее образование в области информационных технологий и профессиональную подготовку в сфере инфраструктуры открытых ключей, а также стаж работы не менее 5 (Пяти) лет в области информационных технологий.
- Инженерно-технические работники УЦ имеют высшее образование в области информационных технологий или профессиональную подготовку в сфере инфраструктуры открытых ключей, необходимой для работы с криптографическими средствами защиты информации.



ПРИЛОЖЕНИЕ №1

Соглашение № _____ о присоединении к Регламенту УЦ

Г. _____

«___» _____ 20__ г.

(наименование лица),
именуемое в дальнейшем «Пользователь», в лице

(должность, ф.и.о. лица, подписывающего договор)

действующего на основании _____

(патента, устава, положения, доверенности N ___ от "___" _____ 20__ г. и т.п.)

и Общество с ограниченной ответственностью «DOS TEK GROUP» (ДОС ТЕК ГРУПП) в лице Генерального Директора Мамбетова Д.Т., действующего на основании устава, именуемое в дальнейшем «УЦ», заключили настоящее соглашение о нижеследующем:

1. В соответствии со статьёй 387 ГК Кыргызской Республики, Пользователь полностью и безоговорочно, присоединяется к Регламенту Удостоверяющего центра общества с ограниченной ответственностью «DOS TEK GROUP» (ДОС ТЕК ГРУПП) условия, которого определены УЦ и опубликованы на информационном портале www.dostek.kg «DOS TEK GROUP» (ДОС ТЕК ГРУПП) в разделе «Удостоверяющий Центр», «Регламент удостоверяющего центра».

2. С Регламентом УЦ и приложениями к нему Пользователь ознакомлен, данные условия принял и обязуется соблюдать все положения указанного документа.

3. Соглашение вступает в силу с момента его подписания сторонами.

4. Адреса и реквизиты сторон:

Пользователь:

УЦ:

Местонахождение: г. Бишкек, ул. Тыныстанова
189 А

Юридический адрес ОсОО «DOS TEK GROUP»
(ДОС ТЕК ГРУПП).: 720014, Кыргызская
Республика, г. Бишкек, ул. Суюмбаева 14 А

Р/с 1280010015061112 ЗАО «Кыргызский
Инвестиционный Кредитный Банк» БИК 128001

Зарегистрировано в УКГНС Октябрьского района
ИНН 00211200910051

Регистрационный номер в Социальном фонде
№04-58756 по Октябрьскому району ОРУСФ 6
мкр., д. 22/1



ПРИЛОЖЕНИЕ №2

Доверенность № _____ на присоединении к Регламенту УЦ

г. _____

« ____ » _____ 20 ____ г.

(наименование лица)
именуемое в дальнейшем «Пользователь», в лице

(должность, ф.и.о. лица, подписывающего договор)

действующего на основании _____,

уполномочивает _____
(должность, фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

подписать соглашение о присоединении к Регламенту УЦ от лица Пользователя, в котором в соответствии со статьёй 387 ГК Кыргызской Республики, Пользователь полностью и безоговорочно, присоединяется к Регламенту Удостоверяющего центра общества с ограниченной ответственностью ОсОО «DOS TEK GROUP» (ДОС ТЕК ГРУПП) условия, которого определены УЦ и опубликованы на информационном портале www.dostek.kg «DOS TEK GROUP» (ДОС ТЕК ГРУПП) в разделе «Удостоверяющий Центр», «Регламент удостоверяющего центра».

Настоящая доверенность действительна по « ____ » _____ 20 ____ г.

Подпись уполномоченного представителя _____ / _____ подтверждаю.
(Фамилия И.О.) (Подпись)

(наименование исполнительного органа, сокращенное наименование пользователя)

(Фамилия И.О.) (Подпись)

М.П.



ПРИЛОЖЕНИЕ №2.1

Доверенность
Пользователя Удостоверяющего центра

Г. _____

« ____ » _____ 20 ____ г.

»,

(наименование лица)

именуемое в дальнейшем «Пользователь», в лице

(должность, ф.и.о. лица, подписывающего договор)

действующего на основании _____,

(патента, устава, положения, доверенности N _____ от " ____ " _____ 20 ____ г. и т.п.)

уполномочивает _____

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1) выступать в роли Пользователя Удостоверяющего центра ОсОО «DOS ТЕК GROUP» (ДОС ТЕК ГРУПП) и осуществлять юридические и фактические действия, предусмотренные в Регламенте Удостоверяющего центра ОсОО «DOS ТЕК GROUP» (ДОС ТЕК ГРУПП) для Пользователя. Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

2) совершать от имени _____

(полное или сокращенное наименование лица)

действия согласно указанным в сертификате ключа подписи Пользователя УЦ областям применения.

Настоящая доверенность действительна по « ____ » _____ 20 ____ г.

Подпись уполномоченного представителя _____ / _____ подтверждаю.
(Фамилия И.О.) (Подпись)

(наименование исполнительного органа, сокращенное наименование пользователя)

(Фамилия И.О.)

(Подпись)

М.П.



ПРИЛОЖЕНИЕ №3

**Заявление на изготовление сертификата ключа подписи пользователя
 физического лица**

(фамилия, имя, отчество)

просит сформировать ключи подписи и изготовить сертификат ключа подписи

(фамилия, имя, отчество) (серия и номер паспорта, кем и когда выдан)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество	
SERIALNUMBER	ИИН физического лица	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	
Extended Key Usage	Проверка подлинности клиента	(1.3.6.1.5.5.7.3.2)
	Защищенная электронная почта	(1.3.6.1.5.5.7.3.4)

Пользователь Удостоверяющего центра

«__» ____ 20__ г.

(Фамилия И.О.)

(Подпись)

М. П.



ПРИЛОЖЕНИЕ №4

Заявление на изготовление сертификата ключа подписи пользователя
юридического лица

(наименование юридического лица)

(должность, фамилия, имя, отчество руководителя юридического лица)

действующий на основании _____

просит сформировать ключи подписи и изготовить сертификат ключа подписи своего
уполномоченного представителя - Пользователя Удостоверяющего центра

(фамилия, имя, отчество) (серия и номер паспорта, кем и когда выдан)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями
использования ключа:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество руководителя организации	
SERIALNUMBER	ИИН юридического лица	
Organization (O)	Наименование организации	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4)

Пользователь Удостоверяющего центра

« ___ » _____ 20 ___ г.

(Фамилия, И.О)

(Подпись)

М. П.



ПРИЛОЖЕНИЕ №5

**Заявление на изготовление сертификата ключа органов
государственной власти и управления**

_____ (наименование органа государственной власти и управления)

_____ (должность, фамилия, имя, отчество руководителя)

действующий на основании _____

просит сформировать ключи подписи и изготовить сертификат ключа подписи своего
уполномоченного представителя - Пользователя Удостоверяющего центра

_____ (фамилия, имя, отчество) (серия и номер паспорта, кем и когда выдан)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями
использования ключа:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество руководителя	
SERIALNUMBER	ИИН органа государственной власти и управления	
Organization (O)	Наименование органа государственной власти и управления	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4)

Пользователь Удостоверяющего центра

«___»_____ 20___ г.

_____ (Фамилия И.О.)

_____ (Подпись)

М. П.



ПРИЛОЖЕНИЕ №6

Заявление**на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра**

_____ (фамилия, имя, отчество пользователя, наименование юридического лица, органа государственной власти и управления)

просит аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра

_____ (фамилия, имя, отчество)

В СВЯЗИ С _____

(прекращение действия, компрометация, устаревание информации)

содержащий следующие идентификационные данные:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество	
Serial Number (SN)	Серийный номер сертификата	
SERIALNUMBER	ИИН	
Organization (O)	Наименование организации	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	

Пользователь Удостоверяющего центра

«___»_____ 20___ г.

_____ (Фамилия И.О.)

_____ (Подпись)

М. П.



ПРИЛОЖЕНИЕ №7

Заявление на приостановление действия сертификата ключа подписи
Пользователя Удостоверяющего центра

(фамилия, имя, отчество пользователя, наименование юридического лица, органа государственной власти и управления)

просит приостановить действие сертификата ключа подписи Пользователя Удостоверяющего центра:

(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество	
Serial Number (SN)	Серийный номер сертификата	
SERIALNUMBER	ИИН	
Organization (O)	Наименование организации	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	

Срок приостановления действия сертификата до «___»_____ 20___ г.

Пользователь Удостоверяющего центра

«___»_____ 20___ г.

(Фамилия И.О.)

(Подпись)

М. П.



ПРИЛОЖЕНИЕ №8

**Заявление на возобновление действия сертификата ключа подписи
Пользователя Удостоверяющего центра**

_____ (фамилия, имя, отчество пользователя, наименование юридического лица, органа государственной власти и управления)

просит возобновить действие сертификата ключа подписи Пользователя Удостоверяющего центра:

_____ (фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество	
Serial Number (SN)	Серийный номер сертификата	
SERIALNUMBER	ИИН	
Organization (O)	Наименование организации	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	

Пользователь Удостоверяющего центра

«___» _____ 20___ г.

_____ (Фамилия И.О.)

_____ (Подпись)

М. П.



ПРИЛОЖЕНИЕ №9

**Заявление на получении статуса сертификата ключа подписи
Пользователя Удостоверяющего центра**

_____ (фамилия, имя, отчество пользователя, наименование юридического лица, органа государственной власти и управления)

просит предоставить информацию о статусе сертификата ключа подписи Пользователя Удостоверяющего центра:

_____ (фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Поля сертификата	Описание	Данные пользователя
Common Name (CN)	Фамилия, Имя, Отчество	
Serial Number (SN)	Серийный номер сертификата	
SERIALNUMBER	ИИН	
Organization (O)	Наименование организации	
Country (C)	Страна	KG
E-Mail (E)	Адрес электронной почты	

Пользователь Удостоверяющего центра

« ___ » _____ 20 ___ г.

_____ (Фамилия И.О.)

_____ (Подпись)

М. П.

**СЕРТИФИКАТ КЛЮЧА ПОДПИСИ ПУЦ
ОсОО «DOSTEK GROUP» (ДОС ТЕК ГРУПП)**



Центр регистрации юридических лиц

Сертификат ключа подписи

Кому выдан: ПУЦ DOS TEK GROUP (ДОС ТЕК ГРУПП)
Кем выдан: Корневой УЦ КР
Действителен с 22 июня 2010 г. по 22 июня 2017 г.
Версия: V3
Серийный номер: 61 02 D0 D3 00 00 00 00 00 0B
Алгоритм подписи: ГОСТ Р 34.10/34.11-2001
Издатель: Имя: Корневой УЦ КР
 Организация: ГП 'Инфоком'
 Электронная почта: support@infocom.kg
 Страна: KG
Действителен с: 22 июня 2010 г. 15:29:00 (GMT+06:00)
Действителен по: 22 июня 2017 г. 15:38:00 (GMT+06:00)
Владелец: Неструктурированное имя: Уполномоченное лицо - Тарасов Артем Валерьевич
 Имя: ПУЦ DOS TEK GROUP (ДОС ТЕК ГРУПП)
 Подразделение: Подчиненный Удостоверяющий Центр DOS TEK GROUP (ДОС ТЕК ГРУПП)
 Организация: DOS TEK GROUP (ДОС ТЕК ГРУПП)
 Город: Бишкек
 Страна: KG
 Электронная почта: pki@dostek.kg
Открытый ключ: ГОСТ Р 34.10-2001 (512 бит)
 0440 5B07 B1A0 B3AC 1A5A 356B 5F71 43BB 16F3 D665 189E F422 AD56 AB7C 6085 0AEB
 EF95 BF2B 583E 7C4D 64E3 4548 3062 0635 4BE0 1208 6B73 A89C 06F5 B97C 84CF 2B18
 E682
Расширения сертификата X.509
Идентификатор ключа субъекта: C8 EF AB EB 08 2B FF 18 28 6A 60 D1 B4 BC 5D 07 AA 6E F1 5B
Идентификатор ключа центра сертификатов: Идентификатор ключа=27 C8 EF B5 ED 9D 65 0A E1 66 01 71 60 9A F7 BC 32 84 01 2E
Точки распространения списков отзыва (CRL): [1]Точка распространения списка отзыва (COC): Имя точки распространения: Полное имя: URL=http://infocom.kg/cert/27c8efb5ed9d650ae1660171609af7bc3284012e.crl
Использование ключа: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (F6)
Основные ограничения: Тип субъекта=УЦ, ограничение на длину пути=Отсутствует
Результат проверки сертификата: Сертификат действителен. Проверен 25 мая 2011 г. 10:43:01 (GMT+06:00).

Допускается использование в приложениях, оснащенных СКЗИ "Домен-К", ОАО "Инфотекс", г. Москва

Владелец	Оператор Центра регистрации
Подпись	Подпись МП.
« ____ » _____ 201__ г.	« ____ » _____ 201__ г.