

"УТВЕРЖДАЮ"
Директор
ООО «Инфолайн»
_____ Воронин М.М.
«09» января 2007 г.

РЕГЛАМЕНТ
Удостоверяющего Центра Инфолайн

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ.....	4
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	5
1 ВВЕДЕНИЕ.....	7
1.1 Обзорная информация.....	7
1.2 Идентификация.....	7
1.3 Область применения Регламента.....	7
1.4 Контактная информация.....	7
2 ОБЩИЕ ПОЛОЖЕНИЯ.....	7
2.1 Услуги, предоставляемые УЦ.....	7
2.2 Платность услуг.....	8
2.3 Структура сети УЦ.....	8
2.3.1 Центр Управления Сетью.....	8
2.3.2 Удостоверяющий Ключевой Центр.....	8
2.3.3 Группа Администраторов УЦ.....	9
2.3.4 Центры Регистрации.....	9
2.3.5 Клиенты УЦ.....	9
2.3.5.1 Владельцы сертификатов.....	9
2.3.5.2 Пользователи сертификатов открытых ключей ЭЦП.....	9
2.4 Политика конфиденциальности.....	9
2.4.1 Типы конфиденциальной информации.....	9
2.4.2 Типы информации, не относящейся к конфиденциальной.....	10
2.4.3 Исключительные полномочия официальных лиц.....	10
2.5 Разрешение споров.....	10
2.6 Ответственность УЦ.....	10
2.7 Прекращение деятельности УЦ.....	10
3 ОБЯЗАННОСТИ УЧАСТНИКОВ СЕТИ УЦ.....	11
3.1 Обязанности УЦ.....	11
3.2 Обязанности ЦР.....	11

3.3 Обязанности Клиентов.....	11
3.3.1 Обязанности владельцев сертификатов.....	12
3.3.2 Обязанности Доверенных участников.....	12
4 ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ.....	12
4.1 Условия взаимоотношений.....	12
4.2 Порядок подключения к услугам УЦ.....	12
4.2.1 Порядок регистрации.....	12
4.2.2 Первоначальное подключение к сети УЦ.....	13
4.2.3 Формирование ключей ЭЦП и запрос на выдачу сертификата.....	13
4.2.4 Издание и получение сертификата.....	13
4.2.5 Начало работы с сертификатом.....	13
4.3 Плановая смена ключей ЭЦП.....	13
4.4 Приостановление действия, отзыв (аннулирование) сертификата.....	14
4.4.1 Условия приостановления действия и отзывов (аннулирования) сертификатов.....	14
4.4.2 Процедуры по приостановлению действия и отзыву (аннулированию) сертификатов при компрометации ключей.....	14
4.4.3 Процедуры по отзыву (аннулированию) сертификатов.....	15
4.4.4 Приостановка действия.....	15
5 СТРУКТУРА СЕРТИФИКАТА.....	15
5.1 Обязательные поля сертификата.....	15
5.2 Опциональные поля сертификата.....	16
6 РАЗРЕШЕНИЕ СПОРОВ И КОНФЛИКТНЫХ СИТУАЦИЙ.....	16
7 ОСНОВЫ ДЕЯТЕЛЬНОСТИ УЦ.....	16
8 ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ.....	16
9 ПОРЯДОК ОПУБЛИКОВАНИЯ РЕГЛАМЕНТА.....	17
10 Приложение №1. Доверенность	18
11 Приложение №2. Акт уничтожения криптографических ключей	19
12 Приложение №3. Заявление на сертификат ЭЦП	20

Список сокращений

ГА - главный абонент

РФ - Российская Федерация

СОС - список отозванных сертификатов

КЦ - Ключевой Центр

ПО - программное обеспечение

СЗИ – система защиты информации

СКЗИ - средство криптографической защиты информации

СУ - сетевой узел

УКЦ - Удостоверяющий Ключевой Центр

УЦ - Удостоверяющий Центр

ЦУС - Центр Управления Сетью

ЦР - Центр Регистрации

ЭД - электронный документ

ЭДО - электронный документооборот

ЭЦП - электронная цифровая подпись

Термины и определения

Абонент - владелец ключевой дискеты для доступа в сеть УЦ, а также имеющий право формировать и использовать ключи ЭЦП и создавать соответствующий запрос на сертификат.

Аутентификация информации - процедура установления подлинности и целостности информации, содержащейся в документе. Аутентификация может осуществляться как на основе структуры и содержания документа или его реквизитов, так и путем реализации криптографического алгоритма преобразования информации. Доказательная аутентификация информации осуществляется анализом (экспертизой) подписей должностных лиц и печатей на бумажных документах и проверкой правильности электронной цифровой подписи (ЭЦП) для электронных документов при использовании сертифицированных ФСБ (ФАПСИ) средств криптографической защиты информации (СКЗИ).

Владелец сертификата - физическое лицо, на имя которого выдан сертификат открытого ключа ЭЦП и которое владеет соответствующим закрытым ключом ЭЦП.

Клиент сети УЦ (Клиент) – юридическое или физическое лицо, участник ЭДО, заключивший с УЦ Договор на предоставление услуг УЦ и признающий данный Регламент.

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

Зарегистрированный (сертифицированный) открытый ключ - открытый ключ, подписанный ЭЦП ГА УЦ.

Ключевой носитель – носитель, содержащий ключевую и парольную информацию Абонента сети услуг УЦ.

Компрометация ключа - утрата доверия к тому, что используемые секретные ключи недоступны посторонним лицам или подозрение, что секретные ключи были временно доступны неуполномоченным лицам.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, а также настоящим Регламентом.

Конфликтная ситуация - ситуация, при которой возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных СКЗИ.

Корректный электронный документ - электронный документ, прошедший процедуру проверки ЭЦП с подтверждением ее правильности и не имеющий искажений в тексте сообщения, не позволяющих понять его смысл.

Ключ (криптографический ключ) - параметр шифра или его значение, определяющее выбор одного преобразования из совокупности всевозможных, для данного алгоритма преобразований.

Несанкционированный доступ к информации - доступ к информации лиц, не имеющих на то полномочий.

Открытый ключ ЭЦП - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП. Открытый ключ доступен любому Клиенту и предназначен для подтверждения, с использованием СКЗИ, подлинности ЭЦП в электронном документе.

Открытый ключ Клиента является действующим на момент подписания, если он зарегистрирован (сертифицирован) и введен в действие.

Плановая смена ключей - смена ключей, не вызванная компрометацией ключей, в соответствии с документацией на СКЗИ. Производится с периодичностью согласованной с Клиентом, но не превышающей 1-го (одного) года.

Путь сертификации – путь сертификации для конкретного сертификата определяет цепочку связанных сертификатов сети услуг УЦ.

Сеть УЦ - сеть, построенная с использованием технологии виртуальных защищенных сетей, представляющая собой совокупность аппаратно-программных средств защиты информации, включая СКЗИ, и обеспечивающая защиту трафика, передаваемого по каналам открытой сети (интернет) и функции УЦ.

Сертификат открытого ключа (сертификат) - документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица УЦ, который включает в себя открытый ключ ЭЦП Клиента и выдается УЦ Клиенту для подтверждения подлинности открытого ключа и идентификации владельца сертификата открытого ключа;

Секретные (закрытые) ключи - криптографические ключи, которые хранятся Пользователями Системы в тайне. Секретные ключи используются для шифрования документов и формирования ЭЦП Пользователя.

Сетевой узел (СУ) - компьютер, на котором установлено СКЗИ.

Средство криптографической защиты информации (СКЗИ) - программное средство системы защиты информации, используемое для защиты информации в сети УЦ и выполняющее функции по формированию ключей шифрования и ключей ЭЦП, шифрованию и имитозащите данных, и обеспечивает:

- обнаружение случайных или намеренных искажений защищаемой информации, подтверждение ее авторства и подлинности;
- защиту используемых ключей;
- контроль целостности программного обеспечения;
- создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП;
- подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе;
- создание закрытых и открытых ключей ЭЦП.

Список отозванных сертификатов (СОС) - созданный УЦ список сертификатов, отозванных до окончания срока их действия.

Шифрование - процесс преобразования открытой информации с целью сохранения ее в тайне от посторонних лиц при помощи некоторого алгоритма, называемого шифром.

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.

Электронная цифровая подпись (ЭЦП) - набор символов, формируемый из исходного файла при помощи специального алгоритма и содержащий информацию, используемую для проверки целостности файла и идентификации абонента сети услуг УЦ, сформировавшего подпись.

1 ВВЕДЕНИЕ

ООО «Инфолайн» действует как Удостоверяющий Центр (далее по тексту «УЦ»), и является законным ответчиком по всем юридическим вопросам деятельности УЦ.

1.1 Обзорная информация

Настоящий Регламент определяет механизмы предоставления и использования услуг УЦ, включая обязанности пользователей и членов группы администраторов УЦ, процедуры взаимодействия, форматы документов и данных, а также основные организационно-технические меры по обеспечению безопасной работы сети услуг УЦ.

1.2 Идентификация

Наименование документа: «Регламент работы Удостоверяющего Центра Инфолайн».

Версия: 2.

Дата: 01.08.2007 г.

1.3 Область применения Регламента

Настоящий Регламент предназначен для определения сертификационной политики, в соответствии с которой должен функционировать УЦ, а также в определении порядка взаимодействия всех вовлеченных сторон при взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

Сертификационная политика определяет создание, управление и использование цифровых сертификатов открытых ключей ЭЦП (далее по тексту «сертификат») формата X.509 в приложениях, требующих взаимодействия между распределенными компьютерными системами и обеспечения целостности и конфиденциальности электронной информации.

Регламент применим при организации защищенного ЭДО в интересах заинтересованных лиц, принимающих условия получения услуг УЦ.

1.4 Контактная информация

Удостоверяющий Центр:

ООО «Инфолайн»

Почтовый адрес: 185001, г. Петрозаводск, ул. Шотмана, 56

Фактический адрес: 185001, г. Петрозаводск, ул. Шотмана, 56

Телефон: (8142) 77-20-20 Факс: (8142) 77-20-20

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Услуги, предоставляемые УЦ

УЦ в рамках своей сети предоставляет следующие виды услуг:

- изготовление сертификатов;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

- приостановление и возобновление действия сертификатов, а также отзыв (аннулирование) их;
- ведение реестра изготовленных сертификатов;
- проверку уникальности открытых ключей ЭЦП в реестре сертификатов и архиве УЦ;
- выдачу сертификатов в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществление по обращениям владельцев сертификатов подтверждения подлинности ЭЦП в электронном документе в отношении выданных УЦ сертификатов;
- иные, связанные с использованием ЭЦП услуги.

2.2 Платность услуг

Стоимость услуг предоставляемых УЦ определяются согласно действующему в данный период Ценовому Листу УЦ.

2.3 Структура сети УЦ

Сеть услуг УЦ состоит из следующих основных компонент:

- УЦ в составе:
 - Центр Управления Сетью (ЦУС);
 - Удостоверяющий Ключевой Центр (УКЦ);
 - группа администраторов УЦ;
- Центры Регистрации (ЦР);
- Клиенты, подразделяющиеся на две категории:
 - владельцы сертификатов;
 - пользователи сертификатов.

2.3.1 Центр Управления Сетью

ЦУС выполняет следующие функции:

- регистрация СУ;
- распределение задач для СУ;
- регистрация клиентов (абонентов) в сети на СУ;
- задание и изменение разрешенных связей для СУ;
- формирование и рассылка адресных справочников для СУ;
- формирование справочников связей СУ для УКЦ (необходимы для формирования ключевой информации для связываемых СУ);
- рассылка для СУ обновлений справочно-ключевой информации, формируемой УКЦ;
- рассылка для СУ списков отозванных сертификатов и списков сертификатов уполномоченных лиц УЦ своей и смежных сетей;
- прием и передача в УКЦ запросов на сертификаты и обновление сертификатов от абонентов сети, рассылка изданных сертификатов на СУ.

2.3.2 Удостоверяющий Ключевой Центр

УКЦ выполняет следующие функции:

- формирование ключевых дискет для СУ сети услуг УЦ;
- формирование паролей для СУ;
- обновление ключевых дискет;
- создание ключей подписи и издание сертификатов администраторов (Уполномоченных лиц) УЦ;

- ведение справочников сертификатов администраторов УЦ, формирование и отправка в ЦУС обновлений справочников;
- создание ключей подписи абонентов и издание сертификатов по запросам ЦУС;
- рассмотрение запросов на издание сертификатов от абонентов сети;
- хранение информации о запросах и ведение справочников изданных сертификатов;
- рассмотрение запросов на отзыв, приостановление и возобновление сертификатов;
- ведение и отправка в ЦУС для обновления списков отозванных сертификатов.

УЦ обеспечивает возможность формирования и сертификации ключей подписи для алгоритмов ГОСТ Р 34.10-94/34.11-94 и ГОСТ Р 34.10-2001.

2.3.3 Группа Администраторов УЦ

Группа администраторов УЦ выполняет следующие функции:

- реализует функции ЦУС и УКЦ сети УЦ;
- организует и выполняет мероприятия по техническому сопровождению распространяемых СКЗИ и ЭЦП;
- распространяет СКЗИ и ЭЦП.

2.3.4 Центры Регистрации

ЦР входят в организационную структуру сети УЦ, и на основании заключенных Договоров с УЦ выполняют работы по распространению данных услуг на определенной территории.

ЦР выполняют следующие основные поручения УЦ:

- осуществляют деятельность по продвижению и распространению услуг УЦ на определенной территории;
- заключают с клиентами Договора на предоставление услуг от имени УЦ и продлевают их;
- осуществляют взаимодействие с клиентами в соответствии с данным Регламентом;
- осуществляют взаимодействие с УЦ согласно «Регламента взаимодействия сторон по предоставлению услуг УЦ» и «Регламента взаимодействия сторон по предоставлению услуг защиты информации», являющимися неотъемлемой частью Договора между УЦ и ЦР.

2.3.5 Клиенты УЦ

Клиентами УЦ могут быть как физические лица, так и организации (юридические лица) с которыми УЦ (ЦР от имени УЦ) заключил Договор на предоставление услуг от имени УЦ.

2.3.5.1 Владельцы сертификатов

Владельцем сертификата может быть только физическое лицо.

В случае, когда в качестве Клиента выступает юридическое лицо, то его интересы может представлять физическое лицо (Уполномоченный Представитель) при наличии Доверенности, предоставляющей права данному физическому лицу представлять его интересы. Форма Доверенности приведена в Приложении №1 настоящего Регламента.

2.3.5.2 Пользователи сертификатов открытых ключей ЭЦП

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

2.4 Политика конфиденциальности

2.4.1 Типы конфиденциальной информации

Конфиденциальной информацией считается:

- закрытый ключ ЭЦП владельца сертификата, являющегося Клиентом данной сети УЦ;
- персональная и корпоративная информация Клиентов сети УЦ, находящаяся в УЦ и ЦР, не подлежащая непосредственной рассылке в качестве части сертификата, СОС и данного Регламента;
- информация, хранящаяся в журналах аудита ЦУС и УКЦ;
- отчетные материалы по результатам проверок деятельности УЦ, за исключением заключений по результатам проверок, публикуемых в соответствии с настоящим Регламентом.

2.4.2 Типы информации, не относящейся к конфиденциальной

Информация, не относящаяся к конфиденциальной информации, является открытой информацией.

Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации определяется решением УЦ.

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

Также не считается конфиденциальной информация о настоящем Регламенте.

2.4.3 Исключительные полномочия официальных лиц

УЦ не должен раскрывать информацию, относящуюся к конфиденциальной информации, каким бы то ни было сторонним лицам за исключением случаев:

- санкционированных данным Регламентом;
- требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления органов власти РФ.

2.5 Разрешение споров

Сторонами в споре, в случае его возникновения, считаются УЦ и Клиент УЦ.

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

Споры между сторонами не урегулированные в процессе совместных переговоров разрешаются в судебном порядке в соответствии с действующим законодательством РФ.

2.6 Ответственность УЦ

УЦ не несет никакой ответственности в случае нарушения или не соблюдения Клиентами УЦ положений настоящего Регламента.

Ответственность за право Доверенного участника использовать сертификаты владельцев сертификатов, несет сам владелец (Клиент УЦ).

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

2.7 Прекращение деятельности УЦ

Деятельность УЦ может быть прекращена в порядке, установленном законодательством РФ.

В случае прекращения деятельности УЦ реестр УЦ, включающий реестр зарегистрированных пользователей УЦ, реестр изготовленных сертификатов, передаются в архив Уполномоченного Федерального органа.

3 ОБЯЗАННОСТИ УЧАСТНИКОВ СЕТИ УЦ

3.1 Обязанности УЦ

УЦ в своей деятельности руководствуется данным Регламентом, постановлениями органов государственной власти РФ, законом РФ «Об электронной цифровой подписи» и другими законами РФ определяющими деятельность УЦ.

УЦ гарантирует, что все ЦР, действующие от его имени, удовлетворяют соответствующим положениям данного Регламента касательно деятельности ЦР.

УЦ принимает все допустимые меры для ознакомления владельцев и пользователей сертификатов с их правами и обязанностями в плане управления ключевой информацией, сертификатами и программно-аппаратным обеспечением, используемым при работе в рамках сети услуг УЦ.

УЦ обязан:

- публиковать Регламент согласно раздела 9 настоящего Регламента;
- обеспечивать механизмы и процедуры, позволяющие гарантировать, что все ЦР и Клиенты согласны следовать положениям данного Регламента;
- обеспечить работу собственных служб и сервисов сети УЦ, согласующихся с данным Регламентом.

3.2 Обязанности ЦР

ЦР принимает на себя следующие обязательства:

- выполнять поручения УЦ в соответствии с п. 2.3.4 настоящего Регламента;
- выступать представителем УЦ во взаимоотношениях с Клиентами;
- заключать Договоры на предоставление услуг УЦ с Клиентами от имени УЦ;
- доводить до сведения Клиентов всей информации, касающейся прав и обязанностей УЦ, ЦР, владельцев сертификатов и Доверенных участников, содержащейся в данном Регламенте;
- давать консультации по правовым и техническим вопросам, связанным с предоставлением услуг УЦ;
- не заключать договора с Клиентом на предоставление услуг УЦ от своего имени;
- нести ответственность за достоверность сведений о Клиенте, необходимых для изготовления сертификата. ЦР несет гражданскую ответственность перед УЦ за убытки, понесенные УЦ вследствие недостоверности сведений о Клиенте;
- сохранять все документы, полученные от Клиентов, обратившихся за услугами УЦ, в течение оговоренного с УЦ периода, по истечении которого пересылать их в УЦ для дальнейшего хранения.

3.3 Обязанности Клиентов

Клиент обязан выразить согласие с положениями данного Регламента и следовать ему.

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

Клиент обязан хранить в тайне предоставляемую ему при регистрации в сети УЦ (раздел 4.2.1 настоящего Регламента) ключевую и парольную информацию, однозначно идентифицирующую его в сети УЦ.

Клиент несет всю полноту ответственности за действия, производимые в сети УЦ с использованием всей своей ключевой и парольной информации.

Перед тем как использовать сертификат, Клиент должен удостовериться в том, что назначение сертификата соответствует предполагаемому использованию, а также проверить его на действительность с помощью соответствующих функций сертифицированных программных СКЗИ, предоставляемых ЦР при регистрации в сети УЦ и обеспечивающих выполнение такой проверки.

3.3.1 Обязанности владельцев сертификатов

Владелец сертификата обязан:

- защищать закрытые ключи своей ЭЦП, принимать все возможные меры для предотвращения их потери, раскрытия, модификации или несанкционированного использования;
- использовать ключи ЭЦП и сертификаты только для отношений, определенных в соответствующем поле сертификата и согласно настоящему Регламенту;
- производить периодическую (плановую) замену используемых ключей ЭЦП и соответствующего сертификата согласно требованиям раздела 4.3 настоящего Регламента.
- в случае подозрения на компрометацию ключей ЭЦП немедленно оповестить об этом ЦР (УЦ) способом, описанном в разделе 4.4.2 настоящего Регламента.
- уничтожить старые (скомпромитированные) ключи самостоятельно путем физического уничтожения (раздробления, оплавления) ключевых носителей с составлением Акта уничтожения криптографических ключей (Приложение №2) и передачей его в УЦ (ЦР).

3.3.2 Обязанности Доверенных участников

Доверенный участник (пользователь, не являющийся владельцем сертификата) принимает на себя обязанности владельца сертификата.

Перед тем как использовать сертификат, Доверенный Участник должен удостовериться, что назначение сертификата соответствует предполагаемому использованию.

4 ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ

4.1 Условия взаимоотношений

Взаимодействие Клиентов на предмет подключения и дальнейшего обслуживания в рамках сети УЦ производится УЦ или территориальными ЦР.

В случае, если Клиент заключил Договор на предоставление услуг УЦ с территориальным ЦР, то все дальнейшее взаимодействие по получению услуг УЦ производится с этим ЦР, за исключением моментов, требующих непосредственного взаимодействия с УЦ согласно настоящего Регламента.

Получение УЦ любых запросов на действия с сертификатами, не имеющих документального подтверждения необходимости этих действий непосредственно от Клиента или ЦР, не обязывает УЦ производить эти действия.

4.2 Порядок подключения к услугам УЦ

4.2.1 Порядок регистрации

Для подключения к услугам УЦ Клиент заключает с УЦ Договор на предоставление услуг УЦ и производит оплату.

Клиент в соответствии с Договором на предоставление услуг УЦ направляет в УЦ (ЦР) комплект документов согласно Перечню, являющегося непосредственной частью Договора.

В соответствии с графиком подключения к услугам УЦ, Клиенты (сотрудники Клиента), будущие владельцы ключей ЭЦП и соответствующих сертификатов (либо их доверенные лица на основании доверенности), должны:

- пройти процедуру аутентификации личности. Аутентификация личности производится по паспорту или другому документу удостоверяющему личность;
- получить требуемое СКЗИ, техническую документацию и ключевые носители;
- подписать АКТ о получении СКЗИ и ключевых носителей;
- быть проинструктированы специалистами УЦ (ЦР) по правилам работы с СКЗИ и ключевыми носителями.

4.2.2 Первоначальное подключение к сети УЦ

Клиенты (сотрудники Клиента) самостоятельно (или специалисты УЦ (ЦР), если это отдельно оговорено в Договоре на предоставление услуг УЦ) производят все необходимые работы по установке и настройке СКЗИ на выделенном для этого рабочем месте Клиента в соответствии с полученной, по Договору на предоставление услуг УЦ, документацией.

4.2.3 Формирование ключей ЭЦП и запрос на выдачу сертификата

Формирование закрытого и открытого ключей ЭЦП и электронного запроса в УЦ на издание соответствующего сертификата производится Клиентом (владельцем сертификата) на рабочем месте абонента сети УЦ с помощью СКЗИ и в соответствии с Руководством Пользователя на СКЗИ.

Электронный запрос в УЦ на сертификат по умолчанию шифруется и подписывается с помощью установленного СКЗИ и текущих ключей данного СУ.

4.2.4 Издание и получение сертификата

Процедура издания и получения сертификата заключается в следующем:

- Клиент заполняет электронный бланк «Заявления на сертификат ЭЦП» (далее по тексту Заявление) и оформляет его на бумажном носителе в двух экземплярах, заверив их своей рукописной подписью. Бланк Заявления в электронном виде входит в комплект предоставляемых Клиенту документов при подключении к услугам УЦ;
- электронную копию и два экземпляра Заявления на бумажном носителе, Клиент направляет в УЦ или ЦР (см. раздел 4.1);
- УЦ после получения электронного запроса на сертификат от Клиента и его документального подтверждения согласно раздела 4.1, издает и автоматизировано по каналам сети УЦ высылает на рабочее место Клиента изданный сертификат;
- для получения сертификата Клиент (владелец сертификата) должен лично прибыть в УЦ или ЦР (см. раздел 4.1), заверить собственноручной подписью два экземпляра сертификата оформленных на бланках УЦ с содержащимися на них печатью УЦ и подписью уполномоченного лица УЦ, и получить один экземпляр на руки.

4.2.5 Начало работы с сертификатом

Перед использованием сертификата Клиент обязан с помощью СКЗИ и согласно Руководства пользователя на СКЗИ ввести изданный УЦ сертификат в действие, а также проверить статус всех сертификатов согласно их пути сертификации на предмет их действительности.

4.3 Плановая смена ключей ЭЦП

Сроки действия ключей ЭЦП и соответствующего сертификата установлены равными 12 месяцам.

Замена ключей может осуществляться Клиентом (владельцем сертификата) в рамках срока действия текущего сертификата.

Периодическая (плановая) смена используемых ключей ЭЦП и соответствующего сертификата производится Клиентом (владельцем сертификата), на рабочем месте абонента сети УЦ с помощью СКЗИ в соответствии с Руководством Пользователя на СКЗИ.

В случае, если Клиент не произвел плановую смену ключей и сертификата в период его действия (12 месяцев), то замена ключей ЭЦП и соответствующего сертификата должна производиться согласно разделов 4.2.3 и 4.2.4 настоящего Регламента.

4.4 Приостановление действия, отзыв (аннулирование) сертификата

4.4.1 Условия приостановления действия и отзывов (аннулирования) сертификатов

Сертификат должен быть отозван (аннулирован) по следующим причинам:

- отстранение владельца сертификата от выполнения служебных обязанностей;
- компрометация или подозрение на компрометацию закрытого ключа ЭЦП и соответствующего сертификата;
- изменение идентифицирующей информации или атрибутов в сертификате пользователя до истечения срока действия сертификата;
- увольнение владельца сертификата;
- невыполнение владельцем сертификата своих обязательств, согласно условий Договора на предоставление услуг УЦ и настоящего Регламента (возможно только приостановление действия).

Инициатором отзыва (аннулирования) сертификата и приостановления действия в случае компрометации является владелец сертификата.

Инициатором приостановки действия и/или отзыва (аннулирования) сертификата, в случае невыполнения владельцем сертификата своих обязательств, может быть ЦР и/или собственно УЦ.

Информация об приостановленных и отозванных (аннулированных) сертификатах заносится УЦ в СОС, который автоматизировано по каналам сети УЦ распространяется среди участников защищенного ЭДО.

4.4.2 Процедуры по приостановлению действия и отзыву (аннулированию) сертификатов при компрометации ключей

В случае компрометации или подозрения на компрометацию используемых закрытых ключей ЭЦП и соответствующего сертификата, Клиент обязан немедленно оповестить об этом УЦ или территориальный ЦР согласно следующей процедуры:

- Клиент сообщает о факте компрометации по телефону или по электронной почте в УЦ или территориальный ЦР;
- УЦ после получения сообщения о компрометации в течении 4-х часов рабочих часов приостанавливает действие сертификата;
- в течение 24-х часов, с момента сообщения о факте компрометации, Клиент направляет в УЦ или ЦР (см. раздел 4.1) «Уведомление о компрометации секретного ключа ЭЦП» на бумажном носителе, заверив его рукописной подписью владельца сертификата и в электронном виде на носителе данных (дискете). Бланк «Уведомления о компрометации секретного ключа ЭЦП» в электронном виде входит в комплект предоставляемых Клиенту документов при подключении к услугам УЦ;

- УЦ после получения сообщения о компрометации и его документального подтверждения согласно раздела 4.1, аннулирует сертификат Клиента.

В случае, если по истечении 36-ти часов с момента приостановления действия сертификата Клиента, УЦ не получил его документального подтверждения, то действие приостановленного сертификата возобновляется;

- изготовление новых ключей ЭЦП и соответствующего сертификата должно производиться согласно разделам 4.2.3...4.2.4 настоящего Регламента.

4.4.3 Процедуры по отзыву (аннулированию) сертификатов

Действия по отзыву (аннулированию) сертификатов производятся по причинам, оговоренным в разделе 4.4.1 настоящего Регламента, за исключением случая компрометации (см. раздел 4.4.2), согласно следующей процедуры:

- Клиент направляет в УЦ или ЦР (см. раздел 4.1) «Заявку на отзыв сертификата ЭЦП» в электронном виде, заверив ее ЭЦП владельца сертификата, или используя бумажный носитель, заверив его рукописной подписью владельца сертификата. Бланк «Заявки на отзыв сертификата ЭЦП» в электронном виде входит в комплект предоставляемых Клиенту документов при подключении к услугам УЦ;
- Если, согласно раздела 4.1, Клиент взаимодействует с УЦ напрямую, то:
 - УЦ в случае, получения от Клиента документального подтверждения отзыва сертификата, в течение 8-ми рабочих часов отзыва (аннулирует) сертификат;
- Если, согласно раздела 4.1, Клиент взаимодействует с УЦ через ЦР, то:
 - УЦ в случае получения от ЦР электронной копии «Заявки на отзыв Сертификата ЭЦП», заверенной ЭЦП владельца сертификата, в течение 8-ми рабочих часов отзыва (аннулирует) сертификат;
 - УЦ в случае получения сообщения от ЦР о наличии «Заявки на отзыв Сертификата ЭЦП» от Клиента, в течение 8-ми рабочих часов приостанавливает действие сертификата Клиента, а по получению от ЦР оригинала «Заявки на отзыв Сертификата ЭЦП» на бумажном носителе отзыва (аннулирует) сертификат.

4.4.4 Приостановка действия

Период времени, на который УЦ может приостановить действие сертификата Клиента, определяется в каждом конкретном случае индивидуально. Приостановление осуществляется до момента решения всех разногласий по условиям выполнения Клиентом своих обязательств по Договору на предоставление услуг УЦ и настоящего Регламента.

5 СТРУКТУРА СЕРТИФИКАТА

УЦ издает сертификаты абонентов сети услуг УЦ и уполномоченных лиц УЦ как в электронной форме, так и в виде бумажных документов.

5.1 Обязательные поля сертификата

УЦ издает сертификаты, поддерживающие следующие обязательные поля:

Issuer Name	Издатель сертификата
Signature Algorithm Identifier	Алгоритм подписи
Subject Name	Владелец сертификата
Subject Information	Public Key Открытый ключ владельца

Validity (Not Before/After)	Период действия сертификата (Действителен с/Действителен по)
Certificate Serial Number	Серийный номер сертификата

5.2 Опциональные поля сертификата

Сертификаты содержат следующие опциональные поля:

Version	Номер версии
Issuer Unique Identifier	Идентификатор ключа центра сертификатов
Subject Unique Identifier	Идентификатор ключа субъекта
Extensions	Дополнения.

К дополнениям относятся:

Basic Constraints	Основные ограничения
Key Usage	Использование ключа
Extended Key Usage	Расширенное использование ключа
Certificates Policies	Политики применения сертификата
Name Constraints	Ограничения на имена
Subject Key Identifier, Authority Key Identifier	Идентификаторы ключей
Subject Alternative Name, Issuer Alternative Name	Альтернативные имена
CRL Distribution Point, Issuing Distribution Point	Точка распространения списков отзыва
Authority Access Info	Способ доступа к информации УЦ

6 РАЗРЕШЕНИЕ СПОРОВ И КОНФЛИКТНЫХ СИТУАЦИЙ

Между участниками сети УЦ возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭЦП.

Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- нет подтверждения подлинности ЭД средствами проверки ЭЦП получателя;
- оспаривания факта идентификации владельца ЭЦП (владельца сертификата), подписавшего ЭД;
- заявления отправителя или получателя ЭД об его искажении;
- оспаривания факта отправления и/или доставки ЭД;
- оспаривания времени отправления и/или доставки ЭД;
- иные случаи возникновения конфликтных ситуаций.

Для разрешения споров и конфликтных ситуаций участники сети УЦ руководствуются «Порядком разрешения конфликтных ситуаций» входящим в комплект документов по Договору на предоставление услуг УЦ.

7 ОСНОВЫ ДЕЯТЕЛЬНОСТИ УЦ

УЦ имеет необходимые лицензии по всем видам деятельности, связанных с предоставлением услуг по защите информации.

Для обеспечения своей деятельности, УЦ использует СКЗИ сертифицированные в соответствии с действующим законодательством РФ в области защиты информации.

Организационно-техническая структура сети УЦ функционирует в рамках принятой Политики безопасности УЦ.

Все меры по защите информации в УЦ введены в действие распоряжением руководителя УЦ.

8 ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

Оригинал Регламента составляется в бумажной форме и заверяется собственноручной подписью руководителя УЦ и печатью УЦ.

Ошибки или предложения по уточнению положений настоящего Регламента должны направляться в УЦ или территориальный ЦР согласно контактной информации представленной в разделе 1.4 настоящего Регламента.

Изменения в разделы настоящего Регламента, которые по оценкам УЦ не оказывают, либо оказывают незначительное влияние на работу Клиентов сети УЦ, вносятся без изменения номера версии данного документа и оповещения Клиентов.

Изменения в разделы настоящего Регламента, которые по оценкам УЦ могут иметь значительное влияние на работу Клиентов сети УЦ, вносятся с увеличением номера версии данного документа и при условии оповещения этих Клиентов.

9 ПОРЯДОК ОПУБЛИКОВАНИЯ РЕГЛАМЕНТА

ЦР от имени УЦ предоставляет Клиентам полную текстовую версию настоящего Регламента в составе пакета документов по Договору на предоставление услуг УЦ.

Распространение Регламента всем запросившим осуществляется УЦ или ЦР по электронной почте.

Приложение №1
к Регламенту Удостоверяющего Центра
от «__» _____ 200__ г.

"УТВЕРЖДАЮ"
Директор
ООО «Инфолайн»
Воронин М.М.
«__» _____ 200__ г.

ДОВЕРЕННОСТЬ №

Дата выдачи «__» _____ 200__ г..

Доверенность действительна до «__» _____ 200__ г. без права передоверия.

Настоящей доверенностью _____
Наименование организации

зарегистрированное в _____
Регион/город

свидетельство о регистрации № _____ выдано _____

регистрационной палатой _____
наименование

в лице _____
должность, ФИО.

действующего на основании _____
наименование документа

Уполномочивает _____
ФИО уполномоченного лица

Паспорт № _____ серия _____ выдан _____
дата выдачи, наименование органа МВД

совершать от имени _____
наименование организации

следующие операции:

1. Заключение Договора на предоставление услуг УЦ.
2. Подписать АКТы на получение и получить СКЗИ и ключевые носители.
3. Получить и подписать сертификаты открытых ключей.
4. Пройти обучение и подписать Заключение о допуске к работе с СКЗИ.
5. Расписываться в регистрационных журналах.

Подпись представителя _____

Образец подписи _____
ФИО уполномочиваемого лица

Удостоверяю

Руководитель организации

М.П.

подпись

ФИО

Приложение №2
к Регламенту Удостоверяющего Центра
от «__» _____ 200__ г.

"УТВЕРЖДАЮ"
Директор
ООО «Инфолайн»
Воронин М.М.
«__» _____ 200__ г.

АКТ **Уничтожения криптографических ключей**

Настоящий акт составлен в том, что физически уничтожены ключевые носители (дискеты), содержащие криптографические ключи:

№ номер ключа	Владелец ключа
1.	_____
2.	_____
3.	_____
4.	_____

Копии ключевых носителей в количестве _____ экз. уничтожены.

Сертификаты ключей переданы на архивное хранение

Владелец ключа _____ (Фамилия И.О.)

Руководитель организации _____ (Фамилия И.О.)

М.П. «__» _____ 200__ г.

Заявление на сертификат ЭЦП

В соответствии с Договором № _____ от " ____ " _____ 200__ г. прошу изготовить и выдать мне сертификат ЭЦП, содержащий следующие сведения:

Фамилия, Имя и Отчество	
Должность	
Наименование организации, в которой установлена эта должность	
Место нахождения организации (почтовый адрес)	
Открытый ключ электронной цифровой подписи	
Уникальный регистрационный номер сертификата ключа электронной цифровой подписи	

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи

Домен-КС2

Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение

<ul style="list-style-type: none">• обеспечивает получение идентификации от удаленного компьютера;• подтверждает удаленному компьютеру идентификацию вашего компьютера;• защищает сообщения электронной почты.

Наименование и место нахождения Удостоверяющего Центра

ООО «Инфолайн»	185001, г. Петрозаводск, ул. Шотмана, 56
----------------	--

" ____ " _____ 200__ г.

Подпись: _____ / _____ /

Фамилия И.О.

Без удостоверения организацией недействительно!
--

Собственноручную подпись _____

(должность, фамилия, имя, отчество)

_____ и достоверность указанных в настоящем Заявлении данных

УДОСТОВЕРЯЮ

Наименование организации _____

Должность руководителя организации _____

МП

_____ / _____ /
подпись руководителя Фамилия И.О.

" ____ " _____ 200__ г.