"УТВЕРЖДАЮ"
Генеральный директор
ОАО «ИнфоТеКС Интернет Траст»



Прошин А. Е.
17 февраля 2010 г.

РЕГЛАМЕНТ

Удостоверяющего Центра ОАО «ИнфоТеКС Интернет Траст»

2010

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ 4

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 5

1 ВВЕДЕНИЕ 7

1.1 Обзорная информация 7

1.2 Идентификация Регламента 7

1.3 Публикация Регламента 7

1.4 Область применения Регламента 7

1.5 Контактная информация 7

2 ОБЩИЕ ПОЛОЖЕННИЯ 7

2.1 Услуги, предоставляемые УЦ 7

2.2 Структура УЦ 8
2.2.1 Административные функции 8
2.2.2 Функции регистрации 8
2.2.3 Функции безопасности 8

2.3 Пользователи 9

2.4 Разрешение споров 9

2.5 Возмездность услуг 9

2.6 Прекращение деятельности УЦ 9

3 ПРАВА 9

3.1 Права УЦ 9

3.2 Права пользователей 10

4 ОБЯЗАТЕЛЬСТВА 11

4.1 Обязательства УЦ 11
4.1.1 По аудиту информационной безопасности 11
4.1.2 По работе с ключами ЭЦП Уполномоченного лица УЦ 11
4.1.3 По регистрации пользователей 11
4.1.4 По изготовлению закрытых и открытых ключей подписи пользователей 11
4.1.5 По изготовлению сертификатов 12
4.1.6 По поддержанию актуальности СОС 12
4.1.7 По аннулированию (отзыву) сертификатов 12
4.1.8 По ведению реестра сертификатов 12

4.2 Обязательства пользователя 12
4.2.1 Обязанности лиц, проходящих процедуру регистрации 12
4.2.2 Обязанности владельца сертификата ключей подписи 12
4.2.3 Ответственность пользователя 13

5 ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ 13

5.1 Типы конфиденциальной информации 13

5.2 Типы информации, не относящейся к конфиденциальной 13

5.3 Предоставление конфиденциальной информации 13

6 ПОРЯДОК ВЗАИМОДЕЙСТВИЯ 14

6.1 Регистрация и подключение пользователей 14

6.2 Смена ключей подписи пользователя 14
6.2.1 Плановая смена ключей подписи 14
6.2.2 Внеплановая смена ключей подписи 14
6.2.3 Аннулирование (отзыв) сертификата ключа подписи 14
6.2.4 Приостановление действия сертификата ключа подписи 15
6.2.5 Возобновление действия сертификата ключа подписи 15

6.3 Смена ключей подписи Уполномоченного лица УЦ 15
6.3.1 Плановая смена ключей уполномоченного лица УЦ 15
6.3.2 Внеплановая смена ключей подписи Уполномоченного лица УЦ 15

7 СТРУКТУРА СЕРТИФИКАТА 16

7.1 Базовые поля сертификата ключа подписи 16

7.2 Дополнения сертификата 17

7.3 Поддерживаемые параметры и идентификаторы алгоритмов 17

7.4 Формы имени 17

7.5 Ограничения на имена 18

8 СТРУКТУРА СОС 18

9 РАЗРЕШЕНИЕ СПОРОВ 19

10 ОСНОВЫ ДЕЯТЕЛЬНОСТИ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УЦ 19

11 ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ 19

12 ПРИЛОЖЕНИЯ 20

СПИСОК СОКРАЩЕНИЙ

РФ - Российская Федерация

ПО - программное обеспечение

СЗИ – система защиты информации

СКЗИ - средство криптографической защиты информации

СОС - список отозванных сертификатов

СЭД – система электронного документооборота

УКЦ - Удостоверяющий Ключевой Центр

УЦ - Удостоверяющий Центр

ЦР - Центр Регистрации

ЭД - электронный документ

ЭЦП - электронная цифровая подпись

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Пользователь Удостоверяющего центра (Пользователь) – юридическое или физическое лицо, заключившее с Удостоверяющим центром Договор на предоставление услуг Удостоверяющего центра и признающее настоящий Регламент.

Закрытый ключ электронной цифровой подписи (закрытый ключ ЭЦП) – 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 – электронное сообщение, содержащее необходимую информацию для получения сертификата.

Ключевой носитель – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

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

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ.

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 в соответствии с законодательством РФ.

Открытый ключ электронной цифровой подписи (открытый ключ ЭЦП) – 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 подписи - смена ключей подписи, не вызванная компрометацией ключей подписи, производимая пользователем.

Сертификат ключа подписи (сертификат) - 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 участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

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

Удостоверяющий центр (УЦ) – юридическое лицо, выполняющее функции Удостоверяющего центра предусмотренные Федеральным законом об ЭЦП.

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

Электронный документ (ЭД) - 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) - 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 ВВЕДЕНИЕ

Компания ОАО «ИнфоТеКС Интернет Траст» (далее по тексту ОАО «ИИТ») действует как Удостоверяющий Центр и является ответчиком по всем юридическим вопросам деятельности Удостоверяющего центра.

1.1 Обзорная информация

Настоящий Регламент определяет механизмы предоставления и использования услуг УЦ, включая обязанности УЦ и пользователей («стороны»), процедуры взаимодействия сторон, форматы документов и данных, а также основные организационно-технические меры по обеспечению информационной безопасности при использовании предоставляемых УЦ пользователям ключевой информации и СКЗИ (при необходимости).

1.2 Идентификация Регламента

Наименование документа: «Регламент Удостоверяющего Центра ОАО «ИнфоТеКС Интернет Траст».

Версия: 2.1.

Дата: 17.02.2010 г.

Объектный идентификатор: 1.2.643.3.5.0

1.3 Публикация Регламента

Настоящий Регламент публикуется в электронном виде в репозитарии ОАО «ИИТ» по адресу www.iitrust.ru.

1.4 Область применения Регламента

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

Сертификационная политика определяет создание, управление и использование цифровых сертификатов ключей подписи формата X.509 в приложениях, требующих взаимодействия между распределенными компьютерными системами и обеспечения идентификации владельца сертификата ключа подписи и целостности электронной информации.

1.5 Контактная информация

Удостоверяющий Центр:

ОАО «ИнфоТеКС Интернет Траст» г.Москва:

Почтовый адрес: 127287, Москва, Старый Петровско-Разумовский проезд, дом. 1/23, стр.1.

Юридический адрес: 127287, Москва, Старый Петровско-Разумовский проезд, дом. 1/23, стр.1, этаж 2.

Телефон: (495) 737-93-72 Факс: (495) 737-93-73.

E-mail: supportiit@infotecs.ru

Web: www.iitrust.ru

2 ОБЩИЕ ПОЛОЖЕННИЯ

2.1 Услуги, предоставляемые УЦ

В процессе своей деятельности УЦ предоставляет следующие виды услуг:

- создание ключей ЭЦП по обращению пользователей, с гарантией сохранения в тайне закрытого ключа ЭЦП;
- изготовление сертификатов ключей подписи;
- изготовление сертификатов в форме документов на бумажных носителях;
- приостановление и возобновление действия сертификатов, а также отзыв (аннулирование) их;
- ведение реестра изготовленных сертификатов;
- проверку уникальности открытых ключей подписи в реестре сертификатов и архиве УКЦ;
- осуществление по обращениям владельцев сертификатов подтверждения подлинности ЭЦП в ЭД в отношении выданных УЦ сертификатов;
- иные, связанные с использованием ЭЦП, услуги.

2.2 Структура УЦ

Функционирование УЦ обеспечивается выполнением следующих функций:

- Административные;
- Регистрации;
- Безопасности.

2.2.1 Административные функции

Административные функции УЦ включают:

- управление деятельностью УЦ;
- координация деятельности УЦ и ЦР;
- взаимодействие с пользователями в части разрешения вопросов, связанных с применением СКЗИ, ключей подписи и сертификатов, изготовляемых и/или распространяемых УЦ;
- взаимодействие с пользователями УЦ в части разрешения вопросов, связанных с подтверждением ЭЦП Уполномоченного лица УЦ в сертификатах, изготовленных УЦ в электронной форме, или подтверждения собственноручной подписи Уполномоченного лица УЦ в сертификатах, изготовленных УЦ на бумажном носителе.

2.2.2 Функции регистрации

Функции Регистрации выполняются ЦР и включают:

- заключение Договора на предоставление услуг УЦ от имени УЦ;
- регистрация пользователей УЦ;
- ведение реестра зарегистрированных пользователей УЦ;
- предоставление ключей подписи и сертификатов по обращению пользователей УЦ;
- распространение СКЗИ, предоставляемых пользователям при подключении к услугам УЦ;
- техническое обслуживание СКЗИ, предоставляемых пользователям при подключении к услугам УЦ.
- иное взаимодействие с пользователями в соответствии с настоящим Регламентом.

2.2.3 Функции безопасности

Функции безопасности включают:

- организация и выполнение мероприятий по защите ресурсов УКЦ;
- обеспечение взаимодействия с внешними УЦ, участниками различных СЭД, на основе кросс-сертификации;

- изготовление и предоставление ключей подписи по обращению пользователей;
- изготовление и предоставление сертификатов в электронной форме по обращению пользователей;
- изготовление и предоставление сертификатов на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) сертификатов по обращениям владельцев сертификатов ключей подписи;
- приостановление и возобновление действия сертификатов по обращению владельцев сертификатов ключей подписи;
- предоставление пользователям сведений об аннулированных и приостановленных сертификатах;
- предоставление копий сертификатов в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей;
- техническое обеспечение процедуры подтверждения ЭЦП в ЭД, по обращениям пользователей УЦ;
- техническое обеспечение процедуры подтверждения подлинности ЭЦП Уполномоченного лица УЦ в изготовленных сертификатах, по обращениям пользователей.

2.3 Пользователи

Пользователями УЦ могут быть как физические лица, так и организации (юридические лица) с которыми заключен Договор на предоставление услуг УЦ.

В случае, когда в качестве пользователя выступает юридическое лицо, его интересы представляет физическое лицо, действующее на основании учредительных документов, либо доверенности.

2.4 Разрешение споров

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

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, связанные с действием настоящего Регламента, не урегулированные в процессе совместных переговоров разрешаются в судебном порядке в соответствии с действующим законодательством РФ.

2.5 Возмездность услуг

УЦ предоставляет услуги на платной основе.

2.6 Прекращение деятельности УЦ

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

3 ПРАВА

3.1 Права УЦ

УЦ имеет право:

- отказать в подключении к услугам УЦ и регистрации лицам, подавшим заявку на подключение, с указанием причин отказа;
- отказать в изготовлении сертификата зарегистрированным пользователям, подавшим заявление на его изготовление, с указанием причин отказа;
- отказать в аннулировании (отзыве) сертификата владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае если истек установленный срок действия закрытого ключа ЭЦП, соответствующего ключу подписи в сертификате;
- отказать в приостановлении или возобновлении действия сертификата владельцу сертификата, подавшему заявление на приостановление или возобновление действия сертификата, в случае если истек установленный срок действия закрытого ключа ЭЦП, соответствующего ключу подписи в сертификате;
- аннулировать (отозвать) сертификат пользователя в случае установленного факта компрометации соответствующего закрытого ключа ЭЦП, с уведомлением владельца аннулированного (отозванного) сертификата и указанием обоснованных причин;
- приостановить действие сертификата пользователя с уведомлением владельца приостановленного сертификата ключа подписи и указанием обоснованных причин.

3.2 Права пользователей

Пользователи имеют следующие права:

- обращаться в УЦ для внесения в реестр УЦ регистрационной информации о пользователе с целью в дальнейшем стать владельцем сертификата ключа подписи;
- обращаться в УЦ на предмет получения (приобретения) СКЗИ.
- формировать закрытые и открытые ключи подписи на своем рабочем месте с использованием СКЗИ и программных средств, предоставляемых УЦ;
- обращаться в УЦ для изготовления сертификата;
- использовать предоставляемые УЦ пользователю СКЗИ для формирования запроса в электронной форме в УЦ на изготовление сертификата;
- использовать предоставляемые УЦ пользователю СКЗИ для получения в электронной форме по запросу из УКЦ сертификата и ввода в его в действие;
- получать актуальный СОС;
- получить сертификат Уполномоченного лица УЦ;
- получать копию сертификата в электронной форме, находящегося в реестре сертификатов УЦ;
- применять сертификат Уполномоченного лица УЦ для проверки ЭЦП Уполномоченного лица УЦ в сертификатах, изготовленных УЦ;
- применять копию сертификата в электронной форме для проверки ЭЦП ЭД в соответствии со сведениями, указанными в сертификате;
- применять, полученный из УЦ, СОС для проверки статуса сертификатов;
- обращаться в УЦ за подтверждением подлинности ЭЦП в ЭД;
- обращаться в УЦ за подтверждением подлинности ЭЦП Уполномоченного лица УЦ в изготовленных им сертификатах;
- обращаться в УЦ с заявлениями на:
  - изготовление сертификата ключа подписи;

- аннулирования (отзыва) сертификата ключа подписи (в течение срока действия соответствующего закрытого ключа);
- приостановления действия сертификата ключа подписи (в течение срока действия соответствующего закрытого ключа);
- возобновления действия сертификата ключа подписи (в течение срока действия соответствующего закрытого ключа).

4 ОБЯЗАТЕЛЬСТВА

4.1 Обязательства УЦ

4.1.1 По аудиту информационной безопасности

С целью проверки соответствия деятельности УЦ требованиям настоящего Регламента, а также действующим законодательным, нормативным и правовым актам в области обеспечения информационной безопасности при предоставлении услуг УЦ, организуется постоянный внутренний аудит информационной безопасности.

Результаты аудита информационной безопасности используются для внесения предложений и изменение положений настоящего Регламента, а также служебной документации УЦ по обеспечению информационной безопасности, с целью повышения качества предоставления услуг УЦ.

4.1.2 По работе с ключами ЭЦП Уполномоченного лица УЦ

УЦ обязан использовать для изготовления закрытого ключа ЭЦП Уполномоченного лица УЦ и формирования ЭЦП только СКЗИ, сертифицированные в соответствии с действующим законодательством РФ.

УЦ обязан использовать закрытый ключ подписи Уполномоченного лица УЦ только для подписи издаваемых им сертификатов и СОС.

УЦ обязан принимать меры по защите закрытого ключа ЭЦП Уполномоченного лица УЦ в соответствии с положениями настоящего Регламента.

4.1.3 По регистрации пользователей

УЦ обеспечивает регистрацию пользователей по их заявкам на подключение в соответствии с порядком регистрации, изложенном в настоящем Регламенте.

УЦ обеспечивает уникальность регистрационной информации пользователей, заносимой в реестр УЦ и используемой для идентификации владельцев сертификатов.

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

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

4.1.4 По изготовлению закрытых и открытых ключей подписи пользователей

УЦ обязан изготовить закрытый и открытый ключ подписи зарегистрированному пользователю по его заявлению на сертификат ключа подписи с использованием СКЗИ, сертифицированных в соответствии с действующим законодательством РФ.

УЦ обязан обеспечить сохранение в тайне изготовленного закрытого ключа ЭЦП пользователя, а также конфиденциальность изготовленной ключевой информации до момента передачи пользователю.

4.1.5 По изготовлению сертификатов

УЦ обеспечивает изготовление сертификата зарегистрированному пользователю по его заявлению, в соответствии с форматом и порядком идентификации владельца сертификата ключа подписи, определенным в настоящем Регламенте.

УЦ обязан обеспечить уникальность регистрационных (серийных) номеров изготавливаемых сертификатов пользователей.

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

4.1.6 По поддержанию актуальности СОС

УЦ обязан проводить публикацию СОС в точке распространения.

Полный адрес точки распространения СОС указывается в соответствующем поле сертификата пользователя.

Обновление СОС проводится УЦ по факту аннулирования (отзыва) или приостановления действия любого сертификата.

Период времени с момента аннулирования (отзыва) или приостановления действия сертификата (обновления СОС) до момента публикации в точке распространения не должна превышать 1 час.

Вне зависимости от факта обновления СОС, его публикация в точке распространения производится УЦ не реже одного раза в 12 часов.

4.1.7 По аннулированию (отзыву) сертификатов

УЦ обязан аннулировать (отозвать) сертификат по заявлению его владельца.

УЦ обязан в течение 8 часов с момента получения заявления на отзыв занести сведения об аннулированном (отозванном) сертификате в СОС, с указанием даты, времени занесения и причины отзыва.

Датой и временем аннулирования (отзыва) сертификата признается дата и время формирования СОС с внесенными сведениями об аннулированном (отозванном) сертификате.

4.1.8 По ведению реестра сертификатов

УЦ обязан вести реестр всех изготовленных сертификатов пользователей в течение установленного законодательством РФ срока хранения.

Реестр сертификатов ведется в электронном виде средствами УЦ.

Сертификаты представляются в реестре в форме электронных копий изготовленных сертификатов.

УЦ обязан осуществлять выдачу копий сертификатов в электронной форме по обращениям пользователей.

4.2 Обязательства пользователя

4.2.1 Обязанности лиц, проходящих процедуру регистрации

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

Лица, проходящие процедуру регистрации в УЦ, несут ответственность за достоверность предоставленной регистрационной информации.

4.2.2 Обязанности владельца сертификата ключей подписи

- хранить в тайне закрытый ключ подписи, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
- не использовать для подписи ЭД закрытые ключи подписи, если ему известно, что эти ключи используются или использовались ранее другими неуполномоченными на это лицами.
- немедленно обращаться в УЦ с заявлением на аннулирование (отзыв) сертификата в случае, если ему известно, что эти ключи подписи используются или использовались ранее другими неуполномоченными на это лицами;
- использовать сертификат и соответствующий закрытый ключ подписи только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту.

4.2.3 Ответственность пользователя

Пользователь несет ответственность за достаточность применяемых им мер по защите закрытого ключа подписи от компрометации, потери, уничтожения, изменения или иного неавторизованного использования.

5 ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

5.1 Типы конфиденциальной информации

- Закрытый ключ подписи владельца сертификата ключа подписи, являющегося пользователем УЦ. УЦ не хранит и не архивирует закрытые ключи подписи.
- Пароль, предоставляемый пользователю в процессе прохождения процедуры регистрации.
- Персональная и корпоративная информация пользователей, предоставленная УЦ, не подлежащая непосредственной рассылке в качестве части сертификата открытого ключа ЭЦП и СОС.
- Информация, хранящаяся в журналах аудита УЦ.
- Отчетные материалы по выполненным проверкам деятельности УЦ и аудиту информационной безопасности, за исключением заключений по результатам проверок, публикуемых в соответствии с настоящим Регламентом.

5.2 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.

5.3 Предоставление конфиденциальной информации

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

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

6 ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

6.1 Регистрация и подключение пользователей

Для подключения к услугам УЦ пользователь заключает с УЦ Договор на предоставление услуг УЦ.

После заключения Договора между УЦ и пользователем, владелец сертификата ключа подписи совершает следующие действия:

- оформляет Заявление на сертификат ключа подписи (Приложение 1);
- лично прибывает в ЦР;
- проходит процедуру идентификации личности по паспорту или другому документу удостоверяющего личность;
- получает ключевой(ые) носитель(и);
- подписывает сертификат ключа подписи на бумажном носителе;
- подписывает АКТ приема-передачи.

6.2 Смена ключей подписи пользователя

Сроки действия ключей подписи и соответствующего сертификата пользователя устанавливаются равными 12 месяцам.

6.2.1 Плановая смена ключей подписи

Плановая смена ключей подписи производится пользователем с использованием полученных СКЗИ путем формирования новых закрытого и открытого ключей ЭЦП.

Издание сертификата для вновь сформированного открытого ключа ЭЦП пользователя осуществляется в УЦ при получении от пользователя соответствующего электронного запроса на издание сертификата.

В случае, если пользователь не произвел плановую смену ключей подписи и соответствующего сертификата в период его действия (12 месяцев), то смена ключей ЭЦП и соответствующего сертификата осуществляется путем издания нового сертификата, формирования и передачи пользователю нового ключевого носителя с оформлением соответствующего Акта приема-передачи.

6.2.2 Внеплановая смена ключей подписи

Внеплановая смена ключей подписи производится по инициативе пользователя.

Порядок проведения внеплановой смены ключей подписи пользователя производится пользователем в порядке Плановой смены ключей подписи согласно разделу 6.2.1 настоящего Регламента.

6.2.3 Аннулирование (отзыв) сертификата ключа подписи

Аннулирование (отзыв) сертификата ключа подписи, изготовленного УЦ, осуществляется УЦ по заявлению пользователя на отзыв сертификата ключа подписи.

Заявление на отзыв сертификата ключа подписи представляет собой документ в бумажном виде, заверенный собственноручной подписью пользователя (Приложение 2).

При выполнении УЦ процедуры аннулирования (отзыва) сертификата ключа подписи, отозванный сертификат заносится в СОС УЦ (см. раздел 4.1.7 настоящего Регламента).

УЦ может по собственной инициативе отозвать сертификат ключа подписи пользователя в случае установленного факта компрометации ключа подписи (соответствующего закрытого ключа ЭЦП), с уведомлением владельца отозванного сертификата с указанием обоснованных причин отзыва.

6.2.4 Приостановление действия сертификата ключа подписи

Приостановление действия сертификата ключа подписи, изготовленного УЦ, осуществляется УЦ в следующих случаях:

- по заявлению пользователя на приостановление действия сертификата ключа подписи в бумажном виде, представляющему собой документ, заверенный собственноручной подписью пользователя, (Приложение 3);
- по заявлению пользователя в устной форме в случае компрометации или угрозы компрометации закрытого ключа ЭЦП пользователя.

При устном заявлении на приостановление действия сертификата ключа подписи пользователь должен сообщить идентификационные данные, содержащиеся в сертификате ключа подписи и парольную фразу (определяется при регистрации пользователя).

При выполнении УЦ процедуры приостановления сертификата ключа подписи, приостановленный сертификат заносится в СОС УЦ (см. раздел 4.1.7 настоящего Регламента).

УЦ может по собственной инициативе приостановить действие сертификата ключа подписи пользователя, с уведомлением владельца приостановленного сертификата с указанием причин приостановления действия.

6.2.5 Возобновление действия сертификата ключа подписи

Возобновление действия сертификата ключа подписи, изготовленного УЦ, осуществляется УЦ в следующих случаях:

- по заявлению пользователя на возобновление действия сертификата ключа подписи в бумажном виде, представляющему собой документ, заверенный собственноручной подписью пользователя (Приложение 4);
- при неполучении УЦ по истечении 36-ти часов с момента получения устного заявления пользователя на приостановления действия сертификата подписи его документального подтверждения.

При выполнении УЦ процедуры возобновления действия сертификата ключа подписи, сертификат, действие которого возобновлено, удаляется из СОС УЦ (см. раздел 4.1.8 настоящего Регламента).

6.3 Смена ключей подписи Уполномоченного лица УЦ

Срок действия закрытого ключа ЭЦП Уполномоченного лица УЦ устанавливается равным 12 месяцам. Начало действия закрытого ключа ЭЦП Уполномоченного лица УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа подписи.

6.3.1 Плановая смена ключей уполномоченного лица УЦ

Плановая смена ключей подписи Уполномоченного лица УЦ выполняется в соответствии со сроком действия и не позднее окончания срока действия текущего закрытого ключа ЭЦП Уполномоченного лица УЦ.

Процедура плановой смены ключей подписи Уполномоченного лица УЦ выполняется в порядке, определенном эксплуатационной документацией на программно-аппаратный комплекс УЦ.

6.3.2 Внеплановая смена ключей подписи Уполномоченного лица УЦ

Внеплановая смена ключей подписи Уполномоченного лица УЦ производится в случае компрометации или угрозы компрометации закрытого ключа ЭЦП Уполномоченного лица УЦ.

Процедура по внеплановой смене ключей подписи Уполномоченного лица УЦ выполняется в порядке, определенном эксплуатационной документацией на программно-аппаратный комплекс УЦ.

При выполнении процедуры по внеплановой смене ключей подписи Уполномоченного лица УЦ сертификат скомпрометированного ключа подписи Уполномоченного лица УЦ должен быть аннулирован (отозван) и занесен в СОС УЦ.

7 СТРУКТУРА СЕРТИФИКАТА

Удостоверяющий центр издает сертификаты ключей подписи пользователей УЦКУ и уполномоченного лица Удостоверяющего центра в электронной форме (далее по тексту раздела – сертификаты ключей подписи) формата X.509 версии 3.

7.1 Базовые поля сертификата ключа подписи

Сертификаты ключей подписи содержат следующие базовые поля X.509:

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

7.2 Дополнения сертификата

Сертификаты ключей подписи содержат следующие дополнения:

AuthorityKeyIdentifier	Идентификатор открытого ключа Уполномоченного лица УЦ
SubjectKeyIdentifier	Идентификатор ключа владельца сертификата ключа подписи
ExtendedKeyUsage	Область (области) использования ключа, при которых ЭД с ЭПЦ будет иметь юридическое значение
CRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов ключей подписи, изданных УЦ
KeyUsage	Назначение ключа
Basic Constraints	Определяет принадлежность сертификата ключа подписи УЦ и ограничение длины цепочки сертификатов для подчиненного УЦ

7.3 Поддерживаемые параметры и идентификаторы алгоритмов

УЦ обеспечивает формирование ключей подписи пользователей в соответствии с параметрами:

Алгоритм подписи	**Описание**	**Параметры ключа подписи**	**Описание** OID ISO	**Длина ключа**
ГОСТ Р 34.10-2001	Стандарт ЭЦП, основанный на арифметике эллиптических кривых. OID "1.2.643.2.2.19"	ГОСТ Р 34.10-2001 Параметры по умолчанию	Набор параметров по умолчанию (рекомендуется). OID "1.2.643.2.2. 35.1"	512
		ГОСТ Р 34.10-2001 "Оскар"	Набор параметров "КриптоПРО" (Параметры 2) OID "1.2.643.2.2. 35.2"	
		ГОСТ Р 34.10-2001 Параметры подписи 3	Набор параметров "КриптоПРО" (Параметры 3) OID "1.2.643.2.2. 35.3"	

7.4 Формы имени

В сертификате ключа подписи поля идентификационных данных Уполномоченного лица УЦ и владельца сертификата содержат атрибуты имени формата X.500.

7.5 Ограничения на имена

Обязательными атрибутами поля идентификационных данных Уполномоченного лица УЦ являются:

Common Name	Наименование (псевдоним) УЦ
Title	Должность Уполномоченного лица УЦ
Organization	Наименование организации, являющейся владельцем УЦ
Organization Unit	Наименование подразделения, сотрудником которого является Уполномоченное лицо УЦ
Email	Адрес электронной почты УЦ
Locality	Город или населенный пункт место нахождения организации, являющейся владельцем УЦ
Country	RU
Unstructured Name	Фамилия, Имя, Отчество Уполномоченного лица УЦ

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

Common Name	Фамилия, Имя, Отчество
PostalAddress	Адрес, где зарегистрирован владелец сертификата ключа подписи
Email	Адрес электронной почты
Country	RU

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

Common Name	Фамилия, имя, отчество владельца сертификата ключа подписи
Title	Должность владельца сертификата ключа подписи, установленная для него в организации
Organization	Наименование организации, которую представляет владелец сертификата ключа подписи
PostalAddress	Адрес организации, которую представляет владелец сертификата ключа подписи
Email	Адрес электронной почты
Locality	Город или населенный пункт место нахождения организации владельца сертификата ключа подписи
Country	RU

8 СТРУКТУРА СОС

УЦ издает СОС ключей подписи пользователей УЦ и Уполномоченного лица УЦ в электронной форме формата X.509 версии 2.

9 РАЗРЕШЕНИЕ СПОРОВ

9.1 Сторонами в споре, в случае его возникновения, считаются УЦ и сторона, присоединившаяся к Регламенту.

9.2 При рассмотрении спорных вопросов, связанных с настоящим Регламентом, стороны должны руководствоваться действующим законодательством РФ.

9.3 Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

9.4 Сторона, получившая от другой стороны претензию, обязана в течениие 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.

9.5 Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде в соответствии с действующим законодательством РФ.

10 ОСНОВЫ ДЕЯТЕЛЬНОСТИ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УЦ

УЦ имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг УЦ (см. раздел 2.1 настоящего Регламента).

Система безопасности и защиты информации УЦ создана, предоставлена и поддерживается на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством РФ.

Документы регламентирующие обеспечение мер по защите информации УЦ введены в действие соответствующими приказами.

Для обеспечения деятельности, УЦ использует СКЗИ, сертифицированные в соответствии с действующим законодательством РФ.

11 ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

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

Сообщения об ошибках в положениях настоящего Регламента, а также предложения по уточнению его положений должны направляться в УЦ на основании контактной информации, указанной в разделе 1.4 настоящего Регламента.

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

Изменения в разделы настоящего Регламента, которые по оценкам УЦ могут иметь значительное влияние на работу пользователей, вносятся с увеличением номера версии данного документа и при условии уведомления пользователей надлежащим образом.

12 ПРИЛОЖЕНИЯ

Приложение 1. Заявление на сертификат ключа подписи.

Приложение 2. Заявление на отзыв сертификата ключа подписи

Приложение 3. Заявление на приостановление сертификата ключа подписи

Приложение 4. Заявление на возобновление сертификата ключа подписи

Приложение №1
к Регламенту Удостоверяющего Центра
ОАО «ИнфоТеКС Интернет Траст»
от «____» _____20__ г.

В Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление на сертификат ключа подписи

В соответствии с Договором № _____ прошу изготовить и выдать мне сертификат ЭЦП, содержащий следующие сведения:

Фамилия, Имя и Отчество	
Идентификационный номер (ИНН/КПП организации)	
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

- **обеспечивает получение идентификации от удаленного компьютера;**
- **подтверждает удаленному компьютеру идентификацию вашего компьютера;**
- **защищает сообщения электронной почты.**

Наименование и место нахождения Удостоверяющего Центра

ОАО ИнфоТеКС Интернет Траст
127287, г. Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1

"____" _____ 20__ г. Подпись владельца сертификата: _____

Без удостоверения организацией недействительно!

Собственоручную подпись _____
(должность, фамилия, имя, отчество)
_____ и достоверность указанных в настоящем Заявлении данных

УДОСТОВЕРЯЮ

Должность руководителя организации _____

_____ / _____ /
Фамилия И.О.

МП

"____" _____ 20__ г.

Приложение №2
к Регламенту Удостоверяющего Центра
ОАО «ИнфоТеКС Интернет Траст»
от «____» _____20__ г.

В Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление
на отзыв сертификат ключа подписи

Прошу Вас отозвать и признать недействительным изданный сертификат ключа подписи со следующими реквизитами:

Серийный номер сертификата: _____

Имя владельца сертификата (полностью):_____

_____

Организация: _____

_____

ИНН _____

КПП _____

в связи с _____

_____

От пользователя:

_____ /_____/

подпись Фамилия И.О.

"____" _____ 20__г.

М.П.

Приложение №3

к Регламенту Удостоверяющего Центра

ОАО «ИнфоТеКС Интернет Траст»

от «____» _____20__ г.

В Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление
на приостановление действия сертификата ключа подписи

Прошу Вас приостановить действие изданного сертификата ключа подписи со следующими реквизитами:

Серийный номер сертификата: _____

Имя владельца сертификата (полностью):_____

_____

Организация: _____

ИНН: _____

КПП: _____

_____

в связи с _____

_____

От пользователя:

_____ /_____/

подпись Фамилия И.О.

"____" _____ 20__г.

М.П.

Приложение №4

к Регламенту Удостоверяющего Центра

ОАО «ИнфоТеКС Интернет Траст»

от «____» _____20__ г.

В Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление
на возобновление действия сертификата ключа подписи

Прошу Вас возобновить действие изданного сертификата ключа подписи со следующими реквизитами:

Серийный номер сертификата: _____

Имя владельца сертификата (полностью):_____

_____

Организация: _____

ИНН: _____

КПП: _____

_____

в связи с _____

_____

От пользователя:

_____ /_____/

подпись Фамилия И.О.

"____" _____ 20__г.

М.П.