«УТВЕРЖДАЮ»

Директор
ООО «Гвард-Информ»

Ширяев И. А.

« 01 » июля 2010 г.

РЕГЛАМЕНТ

Удостоверяющего Центра Гвард-Информ PrivateNET

г. Тула

СОДЕРЖАНИЕ

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

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 криптографических алгоритмом 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 выдается (либо уже 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 имитозащиты 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 «Гвард-Информ» 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 Гвард-Информ PrivateNET».

Версия: 2.1.

Дата: 01.07.2010г.

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 «Гвард-Информ»

Адрес: 300041, г. Тула, пр. Ленина, 46 оф. 407

Телефон: (4872) 36-13-00 *Факс*: (4872) 32-55-89

2 ОБЩИЕ ПОЛОЖЕННИЯ

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 договору между УЦ и Клиентом.

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;
- 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 алгоритма 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 Клиенты УЦ

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

2.3.4.1 *Владельцы сертификатов*

Владельцем сертификата может быть только **физическое лицо**.

2.3.4.2 *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, 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.

Персональные данные, включаемые в сертификаты издаваемые УЦ, считаются общедоступными.

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 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;
- обеспечить работу собственных служб и сервисов сети УЦ, согласующихся с данным Регламентом.

3.2 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 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 при регистрации в сети УЦ и обеспечивающих выполнение такой проверки.

3.2.1 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 УЦ.

3.2.2 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.

Получение УЦ любых запросов на действия с сертификатами, не имеющих документального подтверждения необходимости этих действий непосредственно от Клиента, 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 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, должны:

- лично прибыть в УЦ для удостоверения подлинности их личности. Аутентификация личности производится по паспорту или другому документу удостоверяющего личность;
- получить требуемое СКЗИ, техническую документацию и ключевые носители;
- подписать АКТ о получении СКЗИ и/или ключевых носителей;
- быть проинструктированы специалистами УЦ по правилам работы с СКЗИ и ключевыми носителями.

4.2.2 Первоначальное подключение к сети УЦ

Клиенты (сотрудники Клиента) самостоятельно (или специалисты УЦ, 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.

4.3 Удаленная схема выпуска сертификатов

4.3.1 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.

4.3.2 Издание и получение сертификата

Процедура издания и получения сертификата по удаленной схеме заключается в следующем:

- Клиент заполняет электронный бланк «Заявления на выпуск сертификата ключей подписи» (по форме Приложения 1) и оформляет его на бумажном носителе в двух экземплярах, заверив их своей рукописной подписью;
- электронную копию и экземпляр «Заявления на сертификат ЭЦП» на бумажном носителе, Клиент направляет в УЦ;
- УЦ после получения электронного запроса на сертификат от Клиента и его документального подтверждения, издает и автоматизировано по каналам сети УЦ высылает на рабочее место Клиента изданный сертификат;
- для получения сертификата на бумажном носителе владелец сертификата (либо его полномочный представитель при наличии доверенности по форме Приложения 3) должен лично прибыть в УЦ, заверить собственноручной подписью два экземпляра сертификата оформленных на бланках УЦ с содержащейся на них печатью УЦ и подписью уполномоченного лица УЦ, и получить один экземпляр на руки.

4.3.3 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.

Вводить сертификат в действие разрешается только после получения сертификата на бумажном носителе.

4.4 Централизованная схема выпуска сертификатов

4.4.1 Издание, получение и начало работы с сертификатом

Процедура издания и получения сертификата по централизованной схеме заключается в следующем:

- Клиент заполняет «Заявления на изготовление сертификата ключей подписи» (по форме приложения Приложение 2) и оформляет его на бумажном носителе в двух экземплярах, заверив их своей рукописной подписью
- Клиент согласовывает с УЦ время прибытия в офис УЦ;
- Владелец сертификата (либо его полномочный представитель при наличии доверенности по форме Приложения 3) прибывает в УЦ, получает вырабатываемые администратором УЦ на основании «Заявления на изготовление сертификата ключей подписи» ключи ЭЦП на ключевом носителе;
- Администратор УЦ оформляет сертификат ЭЦП на бумажном носителе в двух экземплярах, заверяет их собственноручной подписью и печатью УЦ;
- Владелец сертификата (либо его полномочный представитель при наличии доверенности по форме Приложения 3) заверяет собственноручной подписью два экземпляра сертификата оформленных на бланках УЦ с содержащимися на них печатью УЦ и подписью администратора УЦ, один возвращает администратору УЦ, а второй оставляет себе.
- Клиент, на своем рабочем месте, с помощью СКЗИ и согласно Руководства пользователя на СКЗИ вводит изданный УЦ сертификат в действие, а также проверяет статус всех сертификатов согласно их пути сертификации на предмет их действительности

4.5 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 согласно разделов 4.3. либо 4.4., в зависимости от используемой клиентом схемы выпуска сертификатов.

4.6 Приостановление действия, отзыв (аннулирование) сертификата

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

4.6.1 Условия приостановления действия и отзыва (аннулирования) сертификатов

Сертификат должен быть отозван (аннулирован) по следующим причинам:

- компрометация или подозрение на компрометацию закрытого ключа ЭЦП и соответствующего сертификата;
- изменение идентифицирующей информации занесенной в сертификат, до истечения срока действия 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 либо изменения информации в сертификате является Клиент (как юридическое лицо) либо Владелец сертификата (как физическое лицо).

Инициатором приостановки действия сертификата, в случае невыполнение владельцем сертификата своих обязательств является УЦ.

4.6.2 Приостановление действия сертификата ключа подписи

УЦ приостанавливает действие сертификата ключа подписи в следующих случаях:

- По заявлению Клиента по форме Приложения 6, переданному посредством почтовой или курьерской связи либо факсимильным сообщением
- По заявлению Владельца сертификата ключа подписи по форме Приложения 7 при личном прибытии владельца сертификата в УЦ
- По решению УЦ в случаях компрометации или подозрения в компрометации закрытого ключа подписи Пользователя в том случае, если Владельцу сертификата не было известно о возможном факте компрометации ключей
- По решению УЦ в иных случаях, предусмотренных Договором между УЦ и Клиентом

После получения УЦ заявления на приостановление действия сертификата ключа подписи УЦ осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого заявление было принято УЦ.

При принятии положительного решения УЦ приостанавливает действие сертификата открытого ключа и заносит его в список отозванных сертификатов.

В случае отказа в приостановлении действия сертификата ключа подписи Владелец сертификата (Клиент) уведомляется об этом с указанием причины отклонения заявления.

Период времени, на который может быть приостановлено действие сертификата Клиента по решению УЦ, определяется в каждом конкретном случае индивидуально.

4.6.3 Возобновление действия сертификата ключа подписи

УЦ возобновляет действие сертификата ключа подписи приостановленного по заявлению Клиента (Владельца сертификата) только по заявлению Владельца сертификата.

Подача заявления на возобновление действия сертификата ключа подписи осуществляется Владельцем сертификата по форме Приложения №8 при личном прибытии Владельца сертификата в УЦ либо посредством почтовой или курьерской связи.

Возобновление действия сертификата ключа подписи и выпуск списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, должны быть осуществлены не позднее 5-ти рабочих дней следующих за рабочим днем, в течение которого было подано заявление в УЦ.

В случае отказа в возобновлении действия сертификата ключа подписи УЦ уведомляет об этом Клиента (Владельца сертификата).

Возобновление действия сертификата, приостановленного по решению УЦ, осуществляется после решения всех разногласий, по условиям выполнения Клиентом своих обязательств по Договору на предоставление услуг УЦ и настоящего

Регламента.

4.6.4 Отзыв (аннулирование) сертификата ключа подписи Пользователя

УЦ отзывает (аннулирует) сертификат ключа подписи в следующих случаях:

- В случае прекращения действия настоящего Регламента в отношении Владельца сертификата, в случае прекращения действия Договора между Клиентом и УЦ
- По заявлению Клиента по форме Приложения 4, переданному посредством почтовой или курьерской связи
- По заявлению Владельца сертификата по форме Приложения 5, при личном прибытии Владельца сертификата в УЦ

После получения УЦ заявления на отзыв (аннулирование) сертификата ключа подписи УЦ осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого заявление было принято УЦ.

При принятии положительного решения УЦ приостанавливает действие сертификата открытого ключа и заносит его в список отозванных сертификатов.

В случае отказа в отзыве (аннулировании) сертификата ключа подписи Владелец сертификата уведомляется об этом с указанием причины отклонения заявления.

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 Базовые поля сертификата

УЦ издает сертификаты, поддерживающие следующие базовые поля:

Signature:	Подпись УЦ
Issuer	Отличительное имя УЦ
Validity	Даты начала и окончания срока действия сертификата
Subject	Отличительное имя владельца сертификата
SubjectPublicKeyInformation	Идентификатор алгоритма, значение открытого ключа
Version	Версия сертификата формата X.509 версия 3
SerialNumber	Уникальный серийный номер сертификата в реестре сертификатов открытых ключей УЦ

5.2 Дополнения сертификата

Сертификаты содержат следующие дополнения:

AuthorityKeyIdentifier	Идентификатор ключа издателя сертификата
SubjectKeyIdentifier	Идентификатор ключа владельца сертификата
KeyUsage	Область применения ключа
ExtendedKeyUsage	Расширенная область применения ключа
CRLDistributionPoint	Точка распространения СОС

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.

Порядок разрешения конфликтных ситуаций определяется организатором конкретной информационной системы с привлечением 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 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

Настоящий регламент распространяется в форме электронного документа: по адресу: URL=http://ca.ginf.ru/vipnet/4354/reglament/reglamentPrivateNET.pdf

Приложение №1

Заявление на выпуск сертификата ключа подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице_____

(должность, фамилия, имя, отчество)

действующего на основании _____

Просит выпустить сертификат ключа подписи, согласно удаленной схеме выпуска сертификатов "Регламента Удостоверяющего Центра Гвард-Информ PrivateNET", для своего сотрудника:

_____

(фамилия, имя, отчество)

на основании запроса, содержащего следующие данные:

Создан 9 июля 2010 г. 17:09:51 (GMT+04:00)

Серийный номер запроса
---
00 00 00 00 00 00 00 00 00 00 00 00 11 02 00 02

Владелец открытого ключа

Имя:
Должность:
Подразделение:
Организация:
Город:
Страна:

Начало срока действия
---
1 января 2010 г. 12:00:00 (GMT+04:00)

Окончание срока действия
---
1 января 2011 г. 12:00:00 (GMT+04:00)

Открытый ключ

Алгоритм: ГОСТ Р 34.10-2001
Параметры: ГОСТ Р 34.10-2001 EDH Параметры по умолчанию
Длина ключа: 512
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00

Настоящим_____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных Удостоверяющим центром ООО «Гвард-Информ» и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Владелец сертификата: _____ _____

(подпись) (Фамилия И.О.)

«___» _____ 200__ г.

_____ _____ _____

(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

М.П.

«___» _____ 200__ г.

Приложение № 2

Заявление на изготовление сертификата ключа подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

Просит сформировать ключи подписи и изготовить сертификат ключа подписи, согласно централизованной схеме выпуска сертификатов "Регламента Удостоверяющего Центра Гвард-Информ PrivateNET", для своего сотрудника:

_____

(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными:

Должность	
Фамилия, Имя, Отчество	
Наименование подразделения	
Наименование организации	
Город	
Область	

Настоящим _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных Удостоверяющим центром ООО «Гвард-Информ» и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Владелец сертификата: _____ _____

(подпись) (Фамилия И.О.)

«___» _____ 200__ г.

_____ _____ _____

(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

М.П.

«___» _____ 200__ г.

Приложение № 3

ДОВЕРЕННОСТЬ №_____

Дата выдачи «___» _____ 200__ г.

Действительна по «___» _____ 200__ г.

Я, _____
(ФАМИЛИЯ Имя Отчество Владельца сертификата)

_____
(Должность, название организации)

Паспорт _____ _____
(Серия) (Номер)

Кем выдан _____

Дата выдачи _____

ДОВЕРЯЮ

_____
(ФАМИЛИЯ Имя Отчество)

_____
(Должность, название организации)

Паспорт _____ _____
(Серия) (Номер)

Кем выдан _____

Дата выдачи _____

ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

Предоставить в Удостоверяющий Центр ООО "Гвард-Информ" документы, необходимые для изготовления сертификата на мое имя согласно "Регламенту Удостоверяющего Центра Гвард-Информ PrivateNET";

получить носитель, содержащий:

- сформированные ключи подписи и связанный с ними сертификат ключа подписи, выпущенный на мое имя
- сертификат ключа подписи уполномоченного лица удостоверяющего центра

расписаться за меня в двух экземплярах сертификата ключа подписи на бумажном носителе и других документах;

получить мой экземпляр сертификата ключа подписи на бумажном носителе;

Подпись лица, получившего доверенность _____ _____
(подпись) (Фамилия И.О.)

Подпись лица, выдавшего доверенность _____ _____
(подпись) (Фамилия И.О.)

УДОСТОВЕРЯЮ

_____ _____ _____
(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

М.П.

«___» _____ 200__ г.

Приложение № 4

Заявление Клиента
на аннулирование (отзыв) сертификата ключа подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

просит аннулировать (отозвать) сертификат ключа подписи своего сотрудника, выданного Удостоверяющим центром ООО «Гвард-Информ» согласно "Регламенту Удостоверяющего Центра Гвард-Информ PrivateNET" :

_____

(фамилия, имя, отчество)

Серийный номер сертификата:_____

_____	_____	_____
(Должность руководителя, название организации)	(подпись)	(Фамилия И.О.)

М.П.
«___» _____ 200__ г.

Приложение № 5

Заявление Владельца сертификата на аннулирование (отзыв) сертификата ключа подписи

Я, _____

(фамилия, имя, отчество)

прошу аннулировать (отозвать) сертификат ключа подписи, выданный мне Удостоверяющим центром ООО «Гвард-Информ» согласно "Регламенту Удостоверяющего Центра Гвард-Информ PrivateNET" :

Серийный номер сертификата:_____

Владелец сертификата: _____ _____

(подпись) (Фамилия И.О.)

«___» _____ 200__ г.

Приложение № 6

Заявление Клиента
на приостановление действия сертификата ключа подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

просит приостановить действие сертификата ключа подписи своего сотрудника, выданного Удостоверяющим центром ООО «Гвард-Информ» согласно "Регламенту Удостоверяющего Центра Гвард-Информ PrivateNET" :

_____

(фамилия, имя, отчество)

Серийный номер сертификата:_____

_____ _____ _____

(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

М.П.
«___» _____ 200__ г.

Приложение № 7

Заявление Владельца сертификата на приостановление действия сертификата ключа подписи

Я, _____
(фамилия, имя, отчество)

прошу приостановить действие сертификата ключа подписи выданного мне Удостоверяющим центром ООО «Гвард-Информ» согласно "Регламенту Удостоверяющего Центра Гвард-Информ PrivateNET" :

Серийный номер сертификата:_____

Владелец сертификата: _____ _____
(подпись) (Фамилия И.О.)

«___» _____ 200__ г.

Приложение № 8

Заявление на возобновление действия сертификата ключа подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

просит возобновить действие сертификата ключа подписи Пользователя Удостоверяющего центра ООО «Гвард-Информ»:

_____

(фамилия, имя, отчество)

Серийный номер сертификата:_____

Владелец сертификата: _____ _____

(подпись) (Фамилия И.О.)

«___» _____ 200__ г.

_____ _____ _____

(Должность руководителя, название организации) (подпись) (Фамилия И.О.)

М.П.

«___» _____ 200__ г.