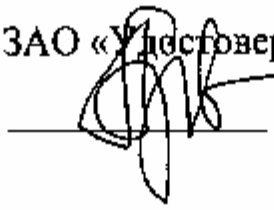
**УТВЕРЖДАЮ**

Генеральный директор

ЗАО «Удостоверяющий центр»



Г.Э. Афанасьев

# РЕГЛАМЕНТ

## изготовления и обслуживания сертификатов открытых ключей Удостоверяющего центра EKEY.ru

Версия: 0.4.1
Дата: 19.11.2007

**Нижний Новгород 2007**

# 1 Введение

Регламент издания и обслуживания сертификатов открытых ключей Удостоверяющим центром ekey.ru, именуемый в дальнейшем Регламент, определяет права и обязанности владельцев сертификатов, а также форматы данных, процедуры работы и организационно-технические мероприятия, реализованные в Удостоверяющем центре ekey.ru при издании и обслуживании сертификатов открытых ключей. Регламент разработан в соответствии с действующим законодательством Российской Федерации и международными рекомендациями. Настоящий регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

## *1.1 Обзорная информация*

Удостоверяющий центр ekey.ru может издавать несколько видов сертификатов открытых ключей. Различные виды сертификатов изготавливаются в рамках различных политик сертификатов и имеют свои области применения. В тексте данного Регламента везде, где есть различия между разными видами сертификатов это указано с приведением конкретных идентификаторов политик. Отдельно отличия различных видов сертификатов и процедур их обслуживания указаны в разделе 7.

## *1.2 Идентификация*

Название документа: «Регламент издания и обслуживания сертификатов открытых ключей Удостоверяющего центра ekey.ru»

Версия: 0.4.1

Дата: 19.11.2007

Данный регламент описывает сертификаты, соответствующие следующим политикам сертификатов (поле Certificate Policies сертификата X509):

- 1.2.643.3.8.100.1
- 1.2.643.3.8.100.1.1
- 1.2.643.3.8.100.1.2
- 1.2.643.3.8.100.1.3
- 1.2.643.3.8.100.1.4
- 1.2.643.6.2.1.7.2
- 1.2.643.6.2.1.7.1

Различия в порядке издания и сферах применения различных видов сертификатов указаны в тексте данного Регламента с приведением конкретных идентификаторов политик.

## *1.3 Присоединение к Регламенту*

Присоединение к Регламенту осуществляется всеми владельцами сертификатов путем подписания договора с обязательным пунктом присоединения к данному Регламенту или Заявления-Соглашения присоединения к Регламенту. Факт присоединения лица к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Подписного листа.

# 2 Общие положения

## *2.1 Удостоверяющий центр ekey.ru*

Услуги Удостоверяющего центра ekey.ru направлены на поддержку защищенных технологий документооборота, электронной коммерции, обмену документами с органами государственной власти, министерствами и ведомствами. Деятельность Удостоверяющего центра ekey.ru направлена на создание единой доверенной системы сервисов на базе инфраструктуры открытых ключей (ИОК).

Удостоверяющий центр ekey.ru в качестве профессионального участника рынка услуг по изданию и выдаче сертификатов ключей подписи осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

лицензия ФАПСИ на право осуществлять деятельность по распространению шифровальных средств № ЛФ/07 - 4333 от 28 мая 2003г.;

лицензия ФАПСИ на право осуществлять предоставление услуг в области шифрования информации № ЛФ/07-4334 от 28 мая 2003г.;

лицензия ФАПСИ на право осуществлять деятельность по техническому обслуживанию шифровальных средств № ЛФ/07-4332 от 28 мая 2003г.)

лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации № 0325 от 5.03. 2005г

**Контактные телефоны, факс:**

- тел./факс (8312) 78-54-09, 78-54-10, 78-54-11

## *2.2 Сертификат ключа подписи*

Сертификат открытого ключа подписи (далее «**Сертификат ключа ЭЦП**») - электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и который предоставляется удостоверяющим центром любому участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации личности владельца сертификата ключа ЭЦП;

Одно физическое лицо может обладать несколькими сертификатами.

## *2.3 Применение сертификатов*

Удостоверяющий центр ekey.ru изготавливает сертификаты, предназначенные для использования в следующих целях: аутентификация, подтверждение авторства (неотрекаемость), шифрование. При этом, сфера использования сертификата может быть дополнительно ограничена. Информация о допустимых сферах применения сертификата указывается для каждого типа сертификатов в самом сертификате. Описание сфер применения сертификатов приводится в данном регламенте в разделе 7, подразделе, соответствующем конкретному типу сертификата.

## *2.4 Финансовые обязательства*

В общем случае финансовая ответственность Удостоверяющего центра ekey.ru перед пользователями сертификатов не превышает суммы, взимаемой за пользование сертификатом.

По желанию владельца сертификата, Удостоверяющий Центр ekey.ru может страховать его финансовую ответственность за возможный ущерб, понесенный в результате "электронного мошенничества".

## *2.5 Контроль за соблюдением регламента.*

В своей деятельности Удостоверяющий Центр ekey.ru опирается на действующую законодательную базу, в которой определены области использования, правила контроля, способы разрешения правовых конфликтов и т.п.:

- Федеральный Закон "Об электронной цифровой подписи"
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
- Гражданский Кодекс Российской Федерации
- (часть первая) от 30.11.1994 N 51-ФЗ (принят Государственной Думой РФ 21.10.1994) (ред. от 15.05.2001) - ст.160, 434.
- (часть вторая) от 26.01.1996 N 14-ФЗ (принят Государственной Думой РФ 22.12.1995) (ред. от 17.12.1999) - ст. 847.

Удостоверяющий Центр ekey.ru оказывает услуги и юридически закрепляет данный факт оформленным должным образом договором или Заявлением-Соглашением с владельцем.

Сами взаимодействующие стороны (пользователи) при обмене между собой заверенными электронными документами должны выразить желание использовать и доверие к технической реализации применяемой технологии ИОК.

# 3 Участники ИОК на базе Удостоверяющего центра ekey.ru

В данном разделе описываются основные компоненты инфраструктуры открытых ключей на базе Удостоверяющего центра ekey.ru. Организационно инфраструктура открытых ключей включает в себя собственно Удостоверяющий центр ekey.ru, который обеспечивает издание сертификатов с использованием Центра сертификации (ЦС), и территориально распределенные Регистрационные Центры (РЦ):

Регистрационные Центры могут являться как подразделениями Удостоверяющего центра ekey.ru, так и сторонними организациями - агентами.

Все клиенты Удостоверяющего центра ekey.ru подразделяются в данном регламенте на две категории:

- владельцы сертификатов,
- пользователи сертификатов.

## *3.1 Центр сертификации*

Центр сертификации (ЦС) Удостоверяющего центра ekey.ru осуществляет:

- издание сертификатов открытых ключей,
- отзыв сертификатов путем включения их в список отозванных сертификатов (СОС),
- ведение базы изданных сертификатов и СОС в течение их срока действия,
- формирование архива всех изданных в ЦС сертификатов.

## *3.2 Регистрационные центры*

Удостоверяющий центр ekey.ru для оказания услуг конечным пользователям взаимодействует с ними через Регистрационные Центры (РЦ). Регистрационные Центры осуществляют:

- принятие запросов на издание сертификатов
- выполнение всех процедур идентификации и аутентификации пользователей
- экспертизу документов, идентифицирующих пользователя и подтверждающих сведения, указываемые в сертификате
- инициируют и подтверждают процедуру обновления, отзыва сертификата.

Регистрационные Центры осуществляют свою деятельность локально, являются представителями Удостоверяющего центра ekey.ru, действуют в рамках партнерства с Удостоверяющим центром ekey.ru, получив необходимые разрешения от Удостоверяющего центра ekey.ru.

## *3.3 Владельцы сертификатов*

Владельцами сертификатов являются физические лица, которые:

- имеют сертификат открытого ключа, изданный Удостоверяющим центром ekey.ru на их имя;
- владеют закрытым ключом, соответствующим открытому ключу, указанному в сертификате.

В случаях, когда сертификаты используются для обеспечения корректной работы каких-либо устройств или программных приложений, должно быть назначено ответственное лицо, на имя которого изготавливается сертификат.

### *3.4 Пользователи сертификатов*

Пользователями сертификатов являются любые физические лица, которые используют сертификаты в соответствии с заданной для них областью применения.

# 4 Технологические аспекты ИОК Удостоверяющего центра ekey.ru

### *4.1 Управление сертификатами*

Удостоверяющий центр ekey.ru выполняет следующие основные функции управления сертификатами:

- Идентификация запрашивающего сертификат.
- Издание сертификата.
- Отзыв сертификата.
- Публикация списка отозванных сертификатов.
- Хранение сертификатов.
- Опубликование сертификатов и информации об их статусе.
- Распространение сертификатов.
- Предоставление сертификатов по запросу

В инфраструктуре открытых ключей на базе Удостоверяющего центра ekey.ru управление сертификатами осуществляет Удостоверяющий центр ekey.ru.

### *4.2 Типы сертификатов*

Удостоверяющий центр ekey.ru предлагает несколько различных типов сертификатов, предназначенных для различных нужд пользователей и ограниченных различными сферами применения. Удостоверяющий центр ekey.ru может расширять типы предоставляемых сертификатов. Различные типы сертификатов, их сферы применения и идентификация описываются в тексте данного регламента.

### *4.3 Наименования и расширения в сертификатах*

#### 4.3.1 Стандарты

При создании сертификатов Удостоверяющий центр ekey.ru ориентируется, но не ограничивается, следующими стандартами:

- X.509, версия 3;
- спецификация IETF/PKIX RFC 2527.
- спецификация IETF/PKIX RFC 3039.
- спецификация IETF/PKIX RFC 3280.
- ГОСТ Р 34.10-2001.

#### 4.3.2 Расширения сертификата

Удостоверяющий центр ekey.ru может изготавливать сертификаты, содержащие расширения согласно стандарту X.509 v.3, а также в соответствии с другими стандартами, например стандартами, используемые Microsoft и Netscape.

Расширение «использование ключа» (key usage OID.2.5.29.15) и «улучшенное использование ключа» (extended key usage OID.2.5.29.37) ограничивают технические способы применения, для которых может использоваться открытый ключ, приведенный в сертификате, и соответствующий ему закрытый.

Расширение «политики сертификата» (certificate policy OID.2.5.29.32) определяет политику, в соответствии с которой издан и эксплуатируется сертификат, и ограничивает сферы применения сертификата, в соответствии с требованиями к уровню доверия и гарантий к данному сертификату, организационными требованиями информационной безопасности; ограничения разрешенных сфер применения сертификатов приведены в описании соответствующей политики.

#### 4.3.3 Политики сертификата

Удостоверяющий центр ekey.ru включает в сертификаты ссылку на политики сертификатов. Соответствующие данной политике условия и ограничения издания и применения сертификатов описаны в этом Регламенте или в отдельных документах.

#### 4.3.4 Соответствие другим документам

Удостоверяющий центр ekey.ru выполняет свою деятельность в соответствии со следующими законами:

- Гражданский кодекс Российской Федерации.
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
- Федеральный закон № 1 от 10 января 2002 года «Об электронной цифровой подписи».

#### 4.3.5 Идентификаторы объектов

Удостоверяющий центр ekey.ru может назначить идентификаторы обьектов (OID) сертификатам, различающимся предъявляемыми к ним требованиями, условиями издания, разрешенными сферами использования, уровнем предоставляемых гарантий. Эти идентификаторы включаются в сертификат как расширение «Политики сертификата» (Certificate policies). Удостоверяющий центр ekey.ru также может размещать в расширении «Политики сертификата» (Certificate policies) указатели, понятные пользователю и показывающие расположение и способ доступа к информации о данной политике, предъявляемыми к сертификатам требованиями, условиями издания, разрешенными сферами использования, уровнем предоставляемых гарантий.

### *4.4 Публикация документов и реестр сертификатов*

#### 4.4.1 Предоставление информации о Регламенте

Полная текстовая версия данного Регламента предоставляется РЦ пользователям при их регистрации.

#### 4.4.2 Предоставление сертификатов и СОС

ЦС Удостоверяющего центра ekey.ru передает сертификаты ключей пользователям по электронной почте или на магнитном носителе (через РЦ). Список отозванных сертификатов публикуется на веб сервере Удостоверяющего центра ekey.ru по адресу: http://ca.ekey.ru/cdp/ekey.crl

#### 4.4.3 Периодичность публикации списка отозванных сертификатов

Обновление СОС производится не реже одного раза в две недели. При необходимости обновление СОС может производиться чаще.

### *4.5 Идентификация владельца сертификата*

До издания сертификата Удостоверяющий центр ekey.ru выполняет процедуры проверки личности владельца сертификата и достоверности сведений, включаемых в сертификат. Непосредственно эти функции выполняют Регистрационные Центры Удостоверяющего Центра ekey.ru, следуя инструкциям, определенным в Удостоверяющем центре ekey.ru в полном соответсвии с данным Регламентом.

### *4.6 Обеспечение безопасности информации*

Безопасность информации в Удостоверяющем центре ekey.ru обеспечивается путем использования только сертифицированных средств защиты информации (в том числе криптографических), реализации необходимых организационно-режимных мер, а также применением для издания сертификатов программного обеспечения, сертифицированного по требованиям ФАПСИ(ФСБ) по уровню «КС1» или «КС2»

### *4.7 Проверка электронной цифровой подписи*

Проверка электронной цифровой подписи производится для проверки того, что:

- Электронная цифровая подпись создана владельцем соответствующего сертификата.
- Подписанное сообщение не было изменено с момента формирования электронной цифровой подписи.

Для проверки электронной цифровой подписи пользователь должен выполнить следующие шаги:

- Определить цепочку сертификатов: необходимо определить цепочку сертификатов от сертификата, используемого для проверки электронной цифровой подписи, до доверенного корневого сертификата.
- Проверить статус сертификата (действительность): необходимо проверить статус сертификата, используемого для проверки электронной цифровой подписи, а также всех сертификатов, входящих в цепочку сертификатов, путем просмотра соответствующих списков отозванных сертификатов.
- Проверка подписанных данных: для проверки электронной цифровой подписи необходимо проверить подпись данных с использованием открытого ключа, представленного в сертификате.
- Проверка сведений, для которых может использоваться сертификат: сфера действия сертификата может быть ограничена.

# 5 Порядок оказания услуг

## *5.1 Требования к лицу, запрашивающему сертификат*

Лицо, запрашивающее сертификат, должно выполнить следующие шаги для запроса сертификата:

- Сгенерировать ключевую пару (открытый и закрытый ключ).
- Создать запрос на сертификат в электронном виде в соответствии с форматом PKCS#10 и написать заявление на издание сертификата (форма заявления в Приложении 1, 2 или 3 к данному регламенту).
- Подписать соглашение присоединения к данному Регламенту или договор на издание и обслуживание сертификата открытого ключа, содержащий пункт о присоединении к данному Регламенту.
- Передать заявку и запрос на сертификат в Регистрационный Центр Удостоверяющего центра ekey.ru.
- Подтвердить свою личность и данные, содержащиеся в запросе на сертификат в соответствии с процедурами, определенными Удостоверяющим центром ekey.ru.

### 5.1.1 Генерация ключевой пары

Лицо, запрашивающее сертификат, несет всю ответственность за генерацию ключей, за соблюдение секретности при генерации ключей и использование соответствующих средств криптографических средств защиты информации. Рекомендуемым носителем закрытого ключа является eToken.

### 5.1.2 Защита закрытого ключа

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

## *5.2 Подтверждение информации, содержащейся в сертификате*

Запросы на сертификат ключа должны подаваться совместно с информацией и документами, подтверждающими сведения, содержащиеся в запросе на сертификат, и личность будущего владельца сертификата.

Удостоверяющий центр ekey.ru может запрашивать дополнительные документы и сведения, если признает это необходимым.

### 5.2.1 Информация и документы, необходимые для издания сертификата ключа физического лица

Информация, необходимая для издания сертификата ключа физического лица перечислена ниже. Удостоверяющий центр ekey.ru может запрашивать дополнительные документы и сведения, если признает это необходимым.

Физическое лицо должно предоставить следующую информацию:

- Адрес электронной почты (в случае, если он будет указан в сертификате).
- Фамилию, имя отчество.
- Почтовый адрес для связи с пользователем.
- Открытый ключ.
- Паспортные данные.
- Информацию об оплате услуг.
- Заявление на издание сертификата ключа подписи с собственноручной подписью, соглашение о присоединении к данному Регламенту.

Физическое лицо должно предоставить совместно с заявлением на издание сертификата ключа подписи свое удостоверение личности (паспорт) и оставить его копию.

### 5.2.2 Информация и документы, необходимые для издания сертификата ключа физического лица с указанием места работы и занимаемой должности

Информация, необходимая для издания сертификата ключа физического лица перечислена ниже. Удостоверяющий центр может запрашивать дополнительные документы и сведения, если признает это необходимым.

Физическое лицо должно предоставить следующую информацию:

- Адрес электронной почты (в случае, если он будет указан в сертификате).
- Фамилию, имя отчество.
- Почтовый адрес для связи с пользователем.
- Открытый ключ.
- Паспортные данные.
- Информацию об оплате услуг.
- Заявление на издание сертификата ключа подписи с собственноручной подписью, соглашение о присоединении к данному Регламенту.
- Полное и сокращенное наименование организации.
- Наименование занимаемой должности и подразделения.
- Месторасположение организации.

Физическое лицо должно предоставить совместно с заявлением на издание сертификата ключа подписи следующие документы, заверенные организацией:

- Копию удостоверения личности (паспорта).
- Копию приказа (протокола, выписку из приказа или протокола) о занимаемой должности.
- Копию свидетельства о постановке организации на налоговый учет.
- Копию устава организации.

Все копии предоставляемых документов должны быть заверены организацией, которая указывается в сертификате. Заявление на издание сертификата должно быть подписано собственноручной подписью владельца сертификата и руководителя организации, указываемой в сертификате.

Физическое лицо должно предоставить совместно с заявлением на издание сертификата ключа подписи свое удостоверение личности (паспорт) и оставить его копию.

В случае единовременной подачи запросов на издания сертификатов ключей сотрудникам одной организации, допускается предоставлять один экземпляр документов, подтверждающих сведения об организации.

## 5.3 Требования для проверки запросов на сертификат

После получения запроса на сертификат Регистрационный центр Удостоверяющего центра ekey.ru проверяет:

- Соответствие данных лица, запрашивающего сертификат лицу, указанным в запросе на сертификат.
- Информация, помещаемая в сертификат соответствует действительности, за исключением непроверяемой информации.
- В случае выполнения запроса на сертификат через доверенных лиц, эти лица имеют на это соответствующие разрешения и права.

Во всех случаях и для всех типов сертификатов владелец сертификата обязан отслеживать точность предоставляемых данных и сообщать обо всех изменениях в Удостоверяющий центр ekey.ru или в Регистрационный центр Удостоверяющего центра ekey.ru.

### 5.3.1 Личное присутствие

Для установления соответствия между лицом, запрашивающим сертификат и открытым ключом, указываемом в сертификате, Удостоверяющий центр ekey.ru может потребовать личное присутствие лица, запрашивающего сертификат, в Регистрационном центре с необходимостью предъявления документов, удостоверяющих личность.

Для сертификатов, изготавливаемых в соответствии с политикой 1.2.643.3.8.100.1 запрос на сертификат может быть передан сотруднику РЦ только лично лицом, запрашивающим сертификат с предоставлением удостоверения личности для обеспечения идентификации лица, подающего запрос на сертификат.

## 5.4 Принятие и отклонение запроса

В случае неуспешной проверки сведений, содержащихся в сертификате, Удостоверяющий центр ekey.ru отклоняет данный запрос на сертификат. Удостоверяющий центр ekey.ru принимает разумные меры для уведомления пользователя об отклонении запроса на сертификат и причинах его отклонения.

Удостоверяющий центр ekey.ru может отклонить запрос на сертификат в случае невыполнения требований данного регламента, а также если это может негативно сказаться на имидже Удостоверяющего центра ekey.ru или нанести какой-либо иной ущерб Удостоверяющему центру ekey.ru или его партнерам.

## 5.5 Согласие пользователя на издание и публикацию сертификата

Издание сертификата производится на основе заявления, подписанного собственноручной подписью лица, запрашивающего сертификат.

## 5.6 Принятие сертификата пользователем

Пользователь принимает изданный сертификат, расписываясь на бумажном экземпляре сертификата. Сертификат считается принятым владельцем сертификата по умолчанию, если Удостоверяющим центром ekey.ru не получено уведомлений о неточностях в сертификате до первого использования сертификата.

Принятие сертификата владельцем сертификата означает:

- Электронная цифровая подпись, созданная с использованием закрытого ключа, соответствующего открытому ключу, приведенному в сертификате является электронной цифровой подписью владельца сертификата.
- Вся информация, содержащаяся в сертификате понятна владельцу сертификата и соответствует действительности.
- Сертификат не используется для противоправных действий.
- Владелец сертификата соглашается с данным Регламентом и обязуется соблюдать его.
- Владелец сертификата контролирует закрытый ключ, использует совместно с закрытым ключом только доверенные системы и принимает разумные меры для

предотвращения потери, кражи, изменения или неавторизованного использования закрытого ключа.

### 5.7 Публикация изданных сертификатов

После издания сертификата, его копия помещается в реестр сертификатов. Пользователям предоставляется информация о статусе сертификата из реестра сертификатов по запросу. Копия реестра сертификатов размещается в справочнике сертификатов, доступ к которому может быть осуществлен из общедоступной сети.

### 5.8 Доверие к электронной цифровой подписи

Электронная цифровая подпись признается равнозначной собственноручной подписи владельца сертификата при выполнении следующих условий:

- Электронная цифровая подпись сформирована в период действия сертификата.
- Электронная цифровая подпись и цепочка сертификатов успешно проверены.
- Пользователь, проверяющий электронную цифровую подпись, соглашается со всеми положениями данного регламента.
- Электронная цифровая подпись использована в соответствии со сведениями, указанными в сертификате ключа подписи.

### 5.9 Аннулирование сертификата

Удостоверяющий центр ekey.ru аннулирует сертификат пользователя:

- По личному заявлению владельца сертификата;
- По заявлению владельца сертификата;
- В случае, если Удостоверяющему центру ekey.ru стало достоверно известно о прекращении действия документа, на основе которого оформлен сертификат.
- В иных случаях, предусмотренных действующим законодательством РФ

Подача заявления на аннулирование (отзыв) сертификата производится непосредственно владельцем сертификата или покупателем сертификата. В заявлении на аннулирование сертификата должны содержаться следующие сведения:

- ФИО и паспортные данные подающего заявление на аннулирование сертификата,
- Причина аннулирования сертификата,
- Реквизиты сертификата, подлежащего аннулированию,
- Подпись подающего заявление на аннулирование сертификата,
- Печать организации (в случае если заявление оформляется от имени покупателя-юридического лица).

Форма заявления на аннулирование (отзыв) сертификата приведена в приложении 4.

Заявление на аннулирование сертификата ключа подписи передается непосредственно в РЦ или в УЦ лично владельцем сертификата (или представителем покупателя при наличии доверенности с печатью организации).

Заявление на аннулирование сертификата может быть оформлено в электронном виде и подписано ЭЦП. В таком виде заявление может быть направлено в РЦ или УЦ по электронным каналам связи.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

# 6 Правовые аспекты издания сертификата

## *6.1 Информация, обозначаемая ссылками*

Удостоверяющий центр обозначает ссылками следующую информацию в сертификатах:

- Условия и ограничения из данного Регламента,
- Политики применения сертификатов,
- Обязательные и необязательные элементы соответствующих стандартов.

## *6.2 Процедура изменения регламента и политик*

В целях улучшения качества обслуживания пользователей и увеличения степени надежности и доверия, Удостоверяющий центр ekey.ru производит обновления данного регламента и применяемых политик. Эти обновления считаются применимыми ко всем сертификатам, изданным позднее чем через 30 дней даты публикации обновленной версии регламента и содержащихся в нем политик.

### 6.2.1 Версии

Версии обозначаются цифрами, разделенными точками и датой публикации. Незначительные изменения обозначаются изменением цифр после точек.

## *6.3 Доверие к непроверенной электронной цифровой подписи*

Все стороны, доверяющие сертификату, обязаны при проверке электронной цифровой подписи проверять подлинность подписи УЦ под сертификатом и статус сертификата путем поиска его в списке отозванных сертификатов или иным способом, определяемым Удостоверяющим центром ekey.ru. Непроверенная в соответствии со всеми процедурами, определенными в данном регламенте, электронная цифровая подпись, не может считаться подписью, принадлежащей владельцу сертификата. Ответственность за доверие к непроверенной электронной цифровой подписи целиком лежит на пользователе.

## *6.4 Обязанности владельца сертификата*

Если иное не обозначено в данном Регламенте, владелец сертификата обязан:

- Иметь знания и навыки в вопросах использования электронной цифровой подписи и криптографии с открытыми ключами
- При запросе сертификата создать новую ключевую пару, не допуская разглашения закрытого ключа и используя доверенные программные системы и аппаратные устройства
- При запросе сертификата предоставлять достоверную информацию
- При изменении информации, содержащейся в сертификате, немедленно извещать об этом Удостоверяющий центр ekey.ru
- Удостоверяться, что открытый ключ, содержащийся в сертификате, изданном Удостоверяющим центром ekey.ru, соответствует используемому закрытому ключу.
- Прочитать, понять и выполнять все условия настоящего Регламента, соответствующих политик и иных опубликованных документов.
- Использовать сертификат только в соответствии с действующим законодательством и настоящим Регламентом.
- Не использовать сертификат, если содержащаяся в нем информация неверна.
- Не использовать закрытый ключ после истечения срока его действия.
- Не допускать компрометацию, потерю, изменение, несанкционированное уничтожение и принимать все необходимые меры для защиты секретного ключа.
- Соблюдать ограничения использования ключа и сертификата.
- При запросе сертификата избегать использования информации, которая может нарушить закон или законные права других юридических или физических лиц.

### 6.5 Обязанности Удостоверяющего центра ekey.ru

В дополнение к остальным пунктам настоящего Регламента, Удостоверяющий центр ekey.ru обязан:

- Выполнять все положения настоящего Регламента и дополняющих его документов.
- При поступлении запроса от Регистрационного Центра на издание сертификата, издать сертификат в соответствии с положениями данного Регламента.
- При поступлении запроса на отзыв сертификата от Регистрационного Центра отозвать сертификат в соответствии с данным Регламентом.
- Отозвать сертификат при поступлении запроса на отзыв сертификата от лица, имеющего на это право.
- Регулярно публиковать список отозванных сертификатов в соответствии с положениями настоящего Регламента.
- Оповещать пользователей об отзыве сертификатов путем помещения их в список отозванных сертификатов и публикации списка отозванных сертификатов.
- По запросам предоставлять копии настоящего Регламента.

### 6.6 Обязанности Регистрационного Центра

Регистрационный центр ekey.ru обязан:

- Принимать запросы на сертификат в соответствии с положениями настоящего Регламента
- Выполнять все необходимые процедуры по проверки запроса на сертификат, предусмотренные данным Регламентом, тщательно проверять соответствие сведений в запросе на сертификат сведениям, в предъявленных документах
- В случае если данным регламентом требуется личное присутствие при передаче запроса, проверять соответствие лица, предъявляющего запрос, лицу, указанному в запросе на сертификат
- Передать запрос на сертификат в Удостоверяющий центр ekey.
- Записывать все предпринимаемые действия в журнал
- Принимать, проверять и отправлять в Удостоверяющий центр ekey.ru все запросы на отзыв сертификатов в соответствии с установленными процедурами и данным Регламентом.

### 6.7 Политика конфиденциальности

Информация, полученная службами Удостоверяющего центра ekey.ru (в том числе и Регистрационным центром) от пользователя, не включаемая в сертификат, не может быть передана третьим лицам за исключением случаев личного на то желания пользователя или в правовых рамках действующего законодательства.

### 6.8 Использование в ответственных применениях

Сертификаты Удостоверяющего центра и другие оказываемые услуги не предназначены для использования в системах управления ответственными приложениями, таких как атомные реакторы, управление воздушным движением, системы управления вооружением и других, где неисправность или неверное функционирование могут повлечь за собой причинение вреда человеческому здоровью, большие материальные потери или экологические последствия.

## *6.9 Права на интеллектуальную собственность*

### 6.9.1 Права на интеллектуальную собственность сертификатов и списков отозванных сертификатов

Удостоверяющий центр ekey.ru сохраняет за собой все права на сертификаты и списки отозванных сертификатов, изданные Удостоверяющим центром ekey.ru. Удостоверяющий центр ekey.ru предоставляет неэксклюзивное право копировать и распространять сертификаты и списки отозванных сертификатов безвозмездно при выполнении условий, что они распространяются целиком и используются в соответствии с данным Регламентом.

### 6.9.2 Права на интеллектуальную собственность данного Регламента

Все права на данный регламент принадлежат Удостоверяющему центру ekey.ru. Копирование, модификация или использование иным образом любой части данного регламента без письменного разрешения Удостоверяющего центра запрещено.

### 6.9.3 Права на наименования

Покупатели и владельцы сертификатов сохраняют за собой все права на используемые торговые марки и названия, содержащиеся в сертификатах.

### 6.9.4 Интеллектуальные права на ключевую информацию и исходный материал для ключевой информации

Право интеллектуальной собственности на ключевые пары и ключевой материал, используемый при издании ключей, соответствующие изданным сертификатам, принадлежат владельцам данных сертификатов.

## *6.10 Плата за оказываемые услуги*

Удостоверяющий центр ekey.ru и Регистрационный центр ekey.ru могут требовать оплату за оказываемые услуги за услуги издания и обслуживания сертификата. Сумма оплаты определяется тарифами, утвержденными Удостоверяющим центром ekey.ru или договоренностями сторон.

# 7 Сертификаты открытых ключей пользователей

Этот раздел описывает особые требования к сертификатам ключей пользователей.

В настоящий момент Удостоверяющим центром ekey.ru поддерживаются сертификаты типа ekey-ГОСТ. Эти сертификаты идентифицируются политикой сертификатов OID.1.2.643.3.8.100.1. Области юридически значимого применения сертификата индентифицируются наличием политик сертификатов:

- 1.2.643.3.8.100.1.1
- 1.2.643.3.8.100.1.2
- 1.2.643.3.8.100.1.3
- 1.2.643.3.8.100.1.4
- 1.2.643.3.8.100.1.5
- 1.2.643.6.2.1.7.2
- 1.2.643.6.2.1.7.1

соответствующие области описаны в пункте 7.1.3.3.

Для издания сертификатов используются криптографические средства, сертифицированные в соответствии с законодательством Российской Федерации, для обеспечения безопасности информации по уровню «КС1» или «КС2».

## *7.1 Сертификат ключа подписи ekey-ГОСТ*

### 7.1.1 Информация, необходимая для регистрации запроса на сертификат

В случае если сертификат изготавливается на физическое лицо без указания места работы и должности, лицо, запрашивающее сертификат должно предоставить следующую информацию:

- Фамилия, имя, отчество полностью,
- Дата и место рождения, номер общегражданского паспорта или иную информацию, позволяющую однозначно идентифицировать лицо и отличать его от лиц с таким же именем, фамилией и отчеством.

В случае если сертификат изготавливается на физическое лицо с указанием места работы, должности или иной информации, ассоциирующей его с каким-либо юридическим лицом, лицо, запрашивающее сертификат должно предоставить следующую информацию:

- Фамилия, имя, отчество полностью,
- Дата и место рождения, номер общегражданского паспорта или иную информацию, позволяющую однозначно идентифицировать лицо и отличать его от лиц с таким же именем, фамилией и отчеством.
- Полное наименование и организационно-правовой статус юридического лица.
- Дополнительную информацию об организации (регистрационные данные: ИНН, КПП и т.д.).
- Доказательство, что лицо, запрашивающее сертификат имеет отношение к указываемому юридическому лицу.

### 7.1.2 Идентификация

Сертификаты ekey-ГОСТ идентифицируются в поле политики сертификата идентификатором (OID) 1.2.643.3.8.100.1.

### 7.1.3 Профиль сертификата пользователя

| **Поле сертификата** | **OID** | **О**[1] | **К**[2] | **Описание** |
|---|---|---|---|---|
| Version | | 1 | | 2(=X.509 v3) |
| serial number | | 1 | | Уникальное, генерируется Удостоверяющим центром ekey.ru |
| signature algorithm | 1.2.643.2.2.3 | 1 | | ГОСТ Р 34.11/34.10-2001 |
| **Issuer** | | | | |
| commonName | CN | 1 | | CA ekey.ru |
| organizationName | O | 1 | | ЗАО «Удостоверяющий центр» |
| localityName | L | 1 | | Нижний Новгород |
| countryName | C | 1 | | RU |
| Email | E | 1 | | contact@ekey.ru |
| **Validity** | | 1 | | |
| notBefore | | 1 | | Дата и время издания сертификата |
| notAfter | | 1 | | Дата и время окончания срока действия сертификата |
| **Subject** | | | | |
| commonName | CN | 1 | | Фамилия Имя Отчество или Псевдоним владельца сертификата |
| surName | SN | | | Фамилия Имя Отчество владельца сертификата |
| organizationName | O | | | Организация, сотрудником которой является владелец сертификата |

[1] Обязательность: 1 – обязательное
[2] Критичность: 1 – критичное

| | | | | |
|---|---|---|---|---|
| organizationUnit | OU | | | Подразделение |
| Title | T | | | Должность, которую занимает владелец сертификата |
| Locality | L | | | Город или населенный пункт местонахождения владельца сертификата |
| State | S | | | Область/Субъект федерации |
| Country | C | 1 | | RU – страна |
| UnstructuredName | | | | ИНН1-КПП-ИНН2,<br>где ИНН1 – ИНН организации владельца сертификата,<br>ИНН2 – личный ИНН владельца сертификата,<br>КПП – КПП организации владельца сертификата |
| Email | E | | | Адрес электронной почты |
| Issuer Signature Algorithm | | 1 | | Алгоритм подписи издателя сертификата<br>ГОСТ Р 34.11/34.10-2001 |
| Issuer Sign | | 1 | | ЭЦП издателя сертификата в соответствии с ГОСТ Р 34.11/34.10-2001 |
| **Дополнения сертификата** | | | | |
| Key Usage | | 1 | 1 | Использование ключа – неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных |
| Extended Key Usage | | 1 | | Улучшенный ключ |
| Certificate Policies | | 1 | | Обозначает правила выдачи, применения сертификата, а также сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение |
| Subject Key Identifier | | 1 | | Идентификатор ключа владельца сертификата |
| Authority Key Identifier | | 1 | | Идентификатор ключа уполномоченного лица Удостоверяющего центра, на котором пописан данный сертификат |
| CRL Distribution point | | | | Точка распространения списка отозванных сертификатов |

#### 7.1.3.1. Поля сертификата, идентифицирующие издателя

В сертификатах ekey-ГОСТ издатель сертификата идентифицируется полем issuer. Сертификат Удостоверяющего центра ekey.ru, указываемый в поле issuer, издан уполномоченному лицу Удостоверяющего центра ekey.ru. В поле issuer указывается следующая информация:

CN (CommonName) = CA ekey.ru – псевдоним, закрепленный за уполномоченным лицом Удостоверяющего центра ekey.ru,

O (OrganizationName) = ЗАО «Удостоверяющий центр» - название организации-Удостоверяющего центра ekey.ru

L (localityName) = Нижний Новгород – город месторасположения Удостоверяющего центра ekey.ru

C (Country) = RU – код страны расположения Удостоверяющего Центра ekey.ru

E (email) = conact@ekey.ru – адрес электронной почты уполномоченного лица Удостоверяющего центра ekey.ru

#### 7.1.3.2. Поля сертификата, идентифицирующие владельца

В сертификатах ekey-ГОСТ владелец сертификата идентифицируется полем subject. В этом поле указывается следующая информация:

CN (CommonName) – фамилия, имя и отчество или псевдоним владельца сертификата; в качестве разделителя необходимо использовать символ «пробел» (0x20), значение должно совпадать с указанным в удостоверении личности (паспорте). При использовании псевдонима, последний должен ассоциироваться с владельцем сертификата; фамилия, имя и отчество владелеца сертификата в этом случае должно быть указано в поле SN

SN (SurName) – фамилия, имя и отчество владельца сертификата при использовании в качестве CN псевдонима; в качестве разделителя необходимо использовать символ «пробел» (0x20), значение должно совпадать с указанным в удостоверении личности (паспорте).

O (OrganizationName) – название организации, в которой работает владелец сертификата. То, что владелец сертификата является сотрудником данной организации должно быть подтверждено соответствующими документами; название организации должно совпадать с названием, указанных в регистрационных документах организации.

OU (OrganizationUnitName) – название подразделения, в котором работает владелец сертификата; эта информация должна быть подтверждена соответствующими документами.

T (Title) – должность, занимаемая владельцем сертификата в указанной организации; эта информация должны быть подтверждена соответствующими документами.

L (LocalityName) - Город или населенный пункт местонахождения владельца сертификата.

S (State) - Область/Субъект федерации местонахождения владельца сертификата.

UnstructuredName – указывается ИНН организации, КПП организации, ИНН владельца сертификата. Формат поля: <ИНН организации>-<КПП организации>-<ИНН владельца сертификата>. Все сведения должны быть подтверждены соответствующими документами.

E(Email) – адрес электронной почты владельца сертификата, указывается по заявлению владельца сертификата.

#### 7.1.3.3. Определение области юридически значимого применения сертификата

Расширение CertificatePolicies предназначено для определения области юридически значимого применения сертификата. В это поле перечисляются "... сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение ..." (ФЗ «Об ЭЦП», ст.6, п.1, абз.6).

Возможно перечисление следующих значений:

- 1.2.643.3.8.100.1.1 – Общее использование в системах ИОК без права заверения документов.
- 1.2.643.3.8.100.1.2 – Передача различных видов отчетности в государственные органы.
- 1.2.643.3.8.100.1.3 – Оформление взаимных обязательств, соглашений, договоров, актов и т.п.
- 1.2.643.3.8.100.1.4 – Внутрикорпоративный документооборот.
- 1.2.643.3.8.100.1.5 – Использование в системах электронной коммерции.
- 1.2.643.6.2.1.7.2 - Использование физическим лицом в отношениях, связанных с возникновением, исполнением (осуществлением) и прекращением гражданских прав и обязанностей в отношении инвестиционных паев паевых инвестиционных фондов, в том числе отношения, связанные с учетом и/или фиксацией прав на инвестиционные паи паевых инвестиционных фондов.
- 1.2.643.6.2.1.7.1 - Использование единоличным исполнительным органом юридического лица или уполномоченными представителями юридического лица в отношениях, связанных с возникновением, исполнением

(осуществлением) и прекращением гражданских и иных прав и обязанностей в сфере негосударственного пенсионного обеспечения, негосударственного пенсионного страхования, в сфере деятельности паевых инвестиционных фондов, акционерных инвестиционных фондов, профессиональных участников рынка ценных бумаг, а также связанной с обслуживанием указанной деятельности услуг кредитных и иных организаций.

#### 7.1.3.4. Дополнительные поля для сертификата с политикой 1.2.643.6.2.1.7.2

В сертификатах, в которых указывается политика 1.2.643.6.2.1.7.2, дополнительно необходимо наличие следующих полей.

| **Поле сертификата** | **Атрибут в поле сертификата** | **Наименование** | **Комментарий** |
|---|---|---|---|
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.1 | Фамилия | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.2 | Имя | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.3 | Отчество | (при наличии) |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.4 | Дата рождения | В формате: ДД.ММ.ГГГГ |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.5 | Гражданство | Для гражданина Российской Федерации указывается “РОССИЯ”<br>“Для гражданина Российской Федерации указывается “РОССИЯ”. В случае иного гражданства указывается наименование государства.” |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.50.1 | ИНН | При наличии |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.1 | Наименование документа, удостоверяющий личность физического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.2 | Серия документа, удостоверяющий личность физического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.3 | Номер документа, удостоверяющий личность физического лица | |
| SubjectAltName- | OID.1.2.643.6.2.1 | Кем выдан (документ, | |

| | | | |
|---|---|---|---|
| >otherName | .6.2.20.4 | удостоверяющий личность физического лица) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.5 | Дата выдачи документа, удостоверяющий личность физического лица | В формате: ДД.ММ.ГГГГ |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.1 | Страна места жительства (регистрации) | Наименование государства |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.2 | Регион (область) места жительства (регистрации) | Субъект Российской Федерации |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.3 | Район места жительства (регистрации) | При наличии |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.4 | Город места жительства (регистрации) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.5 | Населенный пункт места жительства (регистрации) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.6 | Улица места жительства (регистрации) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.7 | Дом места жительства (регистрации) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.8 | Корпус места жительства (регистрации) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.100.9 | Квартира места жительства (регистрации) | |

#### 7.1.3.5. Дополнительные поля для сертификата с политикой 1.2.643.6.2.1.7.1

В сертификатах, в которых указывается политика 1.2.643.6.2.1.7.1, дополнительно необходимо наличие следующих полей.

| **Поле сертификата** | **Атрибут в поле сертификата** | **Наименование** | **Комментарий** |
|---|---|---|---|
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.1 | Фамилия | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.2 | Имя | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.3 | Отчество | (При наличии) |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.1 | Наименование организации | Полное наименование организации в соответствии с учредительными документами”. |

| | | | |
|---|---|---|---|
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.50.1 | ИНН организации | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.50.2 | ОГРН организации | |
| | | Документ, удостоверяющий личность физического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.1 | Наименование документа, удостоверяющего личность физического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.2 | Серия документа, удостоверяющего личность физического лица | При наличии |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.3 | Номер документа, удостоверяющего личность физического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.4 | Кем выдан (документ, удостоверяющий личность физического лица) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.2.20.5 | Дата выдачи документа, удостоверяющего личность физического лица | В формате: ДД.ММ.ГГГГ |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.20.1 | Наименование документа юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.20.2 | Серия документа юридического лица | Серия бланка документа |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.20.3 | Номер документа юридического лица | Номер бланка документа |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.20.4 | Кем выдан (документ юридического лица) | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.20.5 | Дата выдачи документа юридического лица | В формате: ДД.ММ.ГГГГ |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.1 | Страна места нахождения юридического лица | Наименование государства. |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.2 | Регион (область) места нахождения юридического лица | Субъект Российской Федерации |

| | | | |
|---|---|---|---|
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.3 | Район места нахождения юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.4 | Город места нахождения юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.5 | Населенный пункт места нахождения юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.6 | Улица места нахождения юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.7 | Дом места нахождения юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.8 | Корпус места нахождения юридического лица | |
| SubjectAltName->otherName | OID.1.2.643.6.2.1.6.1.100.9 | Квартира (офис) места нахождения юридического лица | |

# 8 Архивное хранение

## *8.1 Документы, подлежащие архивному хранению*

Архивному хранению подлежат следующие документы Удостоверяющего Центра:

- Аннулированные сертификаты открытых ключей уполномоченного лица Удостоверяющего центра ekey.ru;
- Аннулированные сертификаты владельцев сертификатов ключа подписи Удостоверяющего центра ekey.ru;
- Заявления на сертификат ключа подписи;
- Заявления на аннулирование (отзыв) сертификатов открытых ключей;
- Заявления на приостановление действия сертификатов открытых ключей;
- Заявления на возобновление действия сертификатов открытых ключей;

Документы Удостоверяющего центра ekey.ru на бумажных носителях, в том числе и сертификаты ключа подписи пользователей на бумажном носителе, хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

## *8.2 Срок архивного хранения*

Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов – 5 (Пять) лет.

## *8.3 Уничтожение архивных документов*

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой из числа сотрудников Удостоверяющего центра ekey.ru.

# 9 Разрешение споров

В случае возникновения споров между Удостоверяющим центром, пользователем или (и) владельцем сертификата ключа подписи по вопросам, предусмотренным настоящим Регламентом, Стороны примут меры к разрешению их путем применения примирительных процедур в досудебном порядке. В случае невозможности разрешения вышеуказанных споров путем переговоров Стороны вправе обратиться для разрешения споров в Арбитражный суд Нижегородской области.

# 10 Смена ключа подписи уполномоченного лица Удостоверяющего центра ekey.ru

## *10.1 Плановая смена ключей уполномоченного лица Удостоверяющего Центра*

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица Удостоверяющего Центра выполняется не ранее чем через 2 года и не позднее чем через 3 года после начала действия закрытого ключа уполномоченного лица Удостоверяющего Центра.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего Центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего Центра формирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового открытого ключа и подписывает его электронной цифровой подписью с использованием нового закрытого ключа.

Старый закрытый ключ уполномоченного лица Удостоверяющего Центра используется в течении 1 года с момента изготовления сертификата нового открытого ключа уполномоченного лица Удостоверяющего Центра для формирования списков отозванных сертификатов в электронной форме, изданных Удостоверяющим Центром в период действия старого закрытого ключа уполномоченного лица Удостоверяющего Центра.

## *10.2 Внеплановая смена ключей уполномоченного лица Удостоверяющего Центра*

Внеплановая смена ключей выполняется в случае компрометации закрытого ключа уполномоченного лица Удостоверяющего Центра. Процедура внеплановая смена ключей уполномоченного лица Удостоверяющего Центра выполняется в порядке, определенной процедурой плановой смене ключей уполномоченного лица Удостоверяющего Центра. После выполнения процедуры внеплановой смены ключей уполномоченного лица Удостоверяющего Центра, сертификат открытого ключа уполномоченного лица Удостоверяющего Центра аннулируется (отзывается) путем занесения в список отозванных сертификатов.

# 11 Дополнительные услуги Удостоверяющего центра ekey.ru

Удостоверяющий центр ekey.ru вправе оказывать дополнительные услуги, в числе которых:

## *11.1 Генерация ключевой пары.*

Владелец сертификата может передать право генерации ключевой пары Удостоверяющему центре ekey.ru. В этом случае владельцу сертификата передаются все копии закрытого ключа вместе с сертификатом ключа, о чем подписывается акт.

### *11.2 Консультационные услуги*

Удостоверяющий центр ekey.ru вправе оказывать оплачиваемые и неоплачиваемые услуги пользователям, направленные на развитие ИОК.

# 12 Термины и определения

*Авторство документа* – принадлежность документа одному из участников (Пользователю) системы электронного документооборота. Авторство документа определяется путем аутентификации содержащейся в нем информации.

*Аутентификация информации* - установление 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 алгоритмов 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 средств криптографической защиты информации (СКЗИ).

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

*Пользователь* – физическое лицо, участник информационного обмена электронными документами, признающее данный Регламент, использующий сертификат ключа и полагающееся на него.

*Покупатель* – юридическое или физическое лицо, заключившее договор на издание сертификата ключа владельца сертификата и оплачивающее эти услуги.

*Организация пользователя* – юридическое лицо, сотрудником которой является Пользователь и которая указывается в соответствующих полях сертификата пользователя.

*Внеплановая смена ключей* - смена ключей, вызванная компрометацией ключей.

*Компрометация ключа* - утрата доверия к тому, что используемые секретные ключи недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых дискет или иных носителей ключа;
- утрата ключевых дискет или иных носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации.

*Конфиденциальность информации* - субъективно определяемая характеристика информации, означающая необходимость введения ограничений на круг лиц, имеющих к ней доступ.

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

*Конфликтная ситуация* - ситуация, при которой у пользователей возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

*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.

*Криптографическая защита* - защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

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

*Некорректный электронный документ* - электронный документ, не прошедший процедуры проверки ЭЦП, имеющий искажения в тексте сообщения, не позволяющие понять его смысл.

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

*Обработка информации* – создание, хранение, передача, прием, преобразование и отображение информации.

*Открытый ключ подписи* - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе. Открытый ключ Владельца сертификата является действующим на момент подписания, если он входит в состав действующего не момент подписания сертификата.

*Открытый ключ шифрования* – криптографический ключ, предназначенный для шифрования разового (сеансового) ключа шифрования с целью его передачи адресату по открытым каналам связи или для выработки ключа обмена, предназначенного для шифрования и расшифрования информации. Открытые ключи шифрования могут быть известны всем пользователям системы.

*Плановая смена ключей* - смена ключей, не вызванная компрометацией ключей с периодичностью согласованной с Владельцем сертификата.

*Подтверждение подлинности электронной цифровой подписи в электронном документе* - положительный результат проверки соответствующим средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

*Пользователь* – лицо, использующее сертификаты открытых ключей для каких-либо целей.

*Расшифрование* - процесс преобразования шифрованной информации в открытую при помощи шифра.

*Регистрационный центр* – организация, действующая на основании партнерского договора с Удостоверяющим центром ekey.ru и осуществляющая прием документов от Пользователей и передачу запросов на сертификат Удостоверяющему центру ekey.ru.

*Сертификат открытого ключа* - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра ekey.ru, которые включают в себя открытый ключ (ЭЦП и/или шифрования) и которые выдаются удостоверяющим центром ekey.ru участнику информационной системы для подтверждения подлинности открытого ключа и идентификации владельца сертификата открытого ключа.

*Закрыты ключ* - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи и расшифрования шифрованной информации

*Средства электронной цифровой подписи* - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого

ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

*Управление ключами* - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение, а также издание, выдача и отзыв серитфикатов открытых ключей.

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

*Шифр* - совокупность обратимых преобразований множества возможных открытых данных на множество возможных шифрованных данных, осуществляемых по определенным правилам с применением ключей.

*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)* - 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.

*СОС* – список отозванных сертификатов.

Приложение 1

Пример формы заявления на издание сертификата

**Генеральному директору**
**ЗАО "Удостоверяющий центр"**

_____

От: _____

Паспорт: _____

_____

_____

# ЗАЯВЛЕНИЕ
## на издание сертификата ключа ЭЦП

Прошу Вас издать на мое имя сертификат открытого ключа ЭЦП и зарегистрировать его вреестре сертификатов ключей ЭЦП, указав в сертификате следующие сведения:

Фамилия Имя Отчество(CN - Общее имя)= _____
Населенный пункт (L)=_____
Область (S)=_____
Страна (C)=RU
Организация (O)=_____
Подразделение (OU)=_____
Должность (T)=_____
Электронная почта (E)=

**Открытый ключ:**

Алгоритм: _____
Значение ключа:
_____
_____
_____
_____
_____

**Политики применения сертификатов:**

1.2.643.3.8.100.1 Сертификат типа "ekey-ГОСТ"
1.2.643.3.8.100.1.1 Общее использование в системах ИОК без права заверения финансовых документов
1.2.643.3.8.100.1.2 Передача различных видов отчетности в государственные органы
1.2.643.3.8.100.1.3 Оформление взаимных обязательств, соглашений, договоров, актов и т.п.
1.2.643.3.8.100.1.4 Внутрикорпоративный документооборот
1.2.643.3.8.100.1.5 Использование в системах электронной коммерции

Лицо, запрашивающее сертификат _____/_____
(расшифровка подписи)
"___" _____ 200__г.

Данные о работающем сотруднике, занимаемой им должности, наименовании и местонахождении организации подтверждаю.

**Руководитель организации** _____/_____

"___" _____ 200__г.
М.П.

Приложение 2

Заявления на изготовление сертификата для области применения
OID.1.2.643.6.2.1.7.2

**Генеральному директору**
**ЗАО "Удостоверяющий центр"**
**Г.Э.Афанасьеву**

От: _____
Паспорт: _____
_____
_____

# ЗАЯВЛЕНИЕ
## на изготовление сертификата ключа ЭЦП

Прошу Вас изготовить на мое имя сертификат открытого ключа ЭЦП и зарегистрировать его в реестре сертификатов ключей ЭЦП, указав в сертификате следующие сведения:

Фамилия Имя Отчество (CommonName)=Фамилия Имя Отчество
Фамилия (OID.1.2.643.6.2.1.6.2.1)=Фамилия
Имя (OID.1.2.643.6.2.1.6.2.2)=Имя
Отчество (OID.1.2.643.6.2.1.6.2.3)=Отчество
Дата рождения (OID.1.2.643.6.2.1.6.2.4)=Дата рождения
Гражданство (OID.1.2.643.6.2.1.6.2.5)=Гражданство
ИНН (OID.1.2.643.6.2.1.6.2.50.1)=ИНН заявителя

Документ, удостоверяющий личность
Наименование документа (OID.1.2.643.6.2.1.6.2.20.1)=Наименование документа
Серия (OID.1.2.643.6.2.1.6.2.20.2)=Серия документа
Номер (OID.1.2.643.6.2.1.6.2.20.3)=Номер документа
Кем выдан (OID.1.2.643.6.2.1.6.2.20.4)=Кем выдан документ
Дата выдачи (OID.1.2.643.6.2.1.6.2.20.5)=Дата выдачи документа

Место жительства (регистрации)
Страна (CountryName)=Страна
Регион (StateOrProvinceName)=Регион
Город и/или Населенный пункт (LocalityName)=Город и/или Населенный пункт
Страна (OID.1.2.643.6.2.1.6.2.100.1)=Страна
Регион(область) (OID.1.2.643.6.2.1.6.2.100.2)=Регион(область)
Район (OID.1.2.643.6.2.1.6.2.100.3)=Район
Город (OID.1.2.643.6.2.1.6.2.100.4)=Город
Населенный пункт (OID.1.2.643.6.2.1.6.2.100.5)=Населенный пункт
Улица (OID.1.2.643.6.2.1.6.2.100.6)=Улица
Дом (OID.1.2.643.6.2.1.6.2.100.7)=Дом
Корпус (OID.1.2.643.6.2.1.6.2.100.8)=Корпус
Квартира (OID.1.2.643.6.2.1.6.2.100.9)=Квартира

Электронная почта (Email)=Адрес электронной почты

**Открытый ключ:**
Алгоритм: алгоритм
Значение ключа: значение ключа

**Улучшенное использование ключа:**
1.3.6.1.5.5.7.3.2 Проверка подлинности клиента
1.3.6.1.5.5.7.3.4 Защищенная электронная почта

**Политики применения сертификатов:**
1.2.643.6.2.1.7.2 Отношения, связанные с возникновением, исполнением (осуществлением) и прекращением гражданских прав и обязанностей в отношении инвестиционных паев паевых инвестиционных фондов, в том числе отношения, связанные с учетом и/или фиксацией прав на инвестиционные паи паевых инвестиционных фондов.

Ознакомлен(а) и настоящим заявляю о добровольном принятии мною Правил ЭДО “Личный кабинет. Для владельцев паев”, утвержденных ЗАО “Первый Специализированный Депозитарий”, и регламентирующих отношения, которые указаны в политике применения сертификата ключа подписи. Выражаю согласие с тем, что используемая техническая реализация электронного документооборота достаточна для обеспечения защиты информации от несанкционированного доступа, подтверждения подлинности, авторства электронных документов и разбора конфликтных ситуаций по ним, а также с тем, что документ, подписанный электронной цифровой подписью, которая соответствует данному сертификату ключа подписи, юридически эквивалентен документу на бумажном носителе, заверенному собственноручной подписью.

Подписанием настоящего Заявления заявитель присоединяется к Регламенту изготовления и обслуживания сертификатов открытых ключей Удостоверяющего центра EKEY.ru, утвержденного ЗАО «Удостоверяющий центр», принимает и обязуется исполнять все содержащиеся в нем требования, правила и условия.

Согласен(а) с тем, что мои персональные данные могут обрабатываться, включая публикацию сертификата ключа подписи ЭЦП, содержащего мои персональные данные, в сети Интернет.

Лицо, запрашивающее сертификат _____/_____
(расшифровка подписи)
"___" _____ 200__г.

Заявления на изготовление сертификата для области применения
OID.1.2.643.6.2.1.7.1

**Генеральному директору**
**ЗАО "Удостоверяющий центр"**
**Г.Э.Афанасьеву**

От: _____
Паспорт: _____
_____
_____

# ЗАЯВЛЕНИЕ
## на изготовление сертификата ключа ЭЦП

Прошу Вас изготовить на мое имя сертификат открытого ключа ЭЦП и зарегистрировать его в реестре сертификатов ключей ЭЦП, указав в сертификате следующие сведения:

Фамилия Имя Отчество (CommonName)=Фамилия Имя Отчество
Фамилия (OID.1.2.643.6.2.1.6.2.1)=Фамилия
Имя (OID.1.2.643.6.2.1.6.2.2)=Имя
Отчество (OID.1.2.643.6.2.1.6.2.3)=Отчество

Документ, удостоверяющий личность
Наименование документа (OID.1.2.643.6.2.1.6.2.20.1)=Наименование документа
Серия (OID.1.2.643.6.2.1.6.2.20.2)=Серия документа
Номер (OID.1.2.643.6.2.1.6.2.20.3)=Номер документа
Кем выдан (OID.1.2.643.6.2.1.6.2.20.4)=Кем выдан документ
Дата выдачи (OID.1.2.643.6.2.1.6.2.20.5)=Дата выдачи документа

Наименование организации (OID.1.2.643.6.2.1.6.1.1)=Наименование организации
ИНН организации (OID.1.2.643.6.2.1.6.1.50.1)=ИНН организации
ОГРН организации (OID.1.2.643.6.2.1.6.1.50.2)=ОГРН организации

Документ юридического лица (Организации)
Наименование документа (OID.1.2.643.6.2.1.6.1.20.1)=Наименование документа
Серия (OID.1.2.643.6.2.1.6.1.20.2)=Серия документа
Номер (OID.1.2.643.6.2.1.6.1.20.3)=Номер документа
Кем выдан (OID.1.2.643.6.2.1.6.1.20.4)=Кем выдан документ
Дата выдачи (OID.1.2.643.6.2.1.6.1.20.5)=Дата выдачи документа

Адрес места нахождения юридического лица
Страна (CountryName)=Страна
Регион (StateOrProvinceName)=Регион
Город и/или Населенный пункт (LocalityName)=Город и/или Населенный пункт
Страна (OID.1.2.643.6.2.1.6.1.100.1)=Страна
Регион (область) (OID.1.2.643.6.2.1.6.1.100.2)=Регион(область)
Район (OID.1.2.643.6.2.1.6.1.100.3)=Район
Город (OID.1.2.643.6.2.1.6.1.100.4)=Город
Населенный пункт (OID.1.2.643.6.2.1.6.1.100.5)=Населенный пункт
Улица (OID.1.2.643.6.2.1.6.1.100.6)=Улица
Дом (OID.1.2.643.6.2.1.6.1.100.7)=Дом
Корпус (OID.1.2.643.6.2.1.6.1.100.8)=Корпус
Квартира(офис) (OID.1.2.643.6.2.1.6.1.100.9)=Квартира(офис)

Электронная почта (Email)=Адрес электронной почты

**Открытый ключ:**
Алгоритм: алгоритм
Значение ключа: значение ключа

**Улучшенное использование ключа:**
1.3.6.1.5.5.7.3.2 Проверка подлинности клиента
1.3.6.1.5.5.7.3.4 Защищенная электронная почта

**Политики применения сертификатов:**
1.2.643.6.2.1.7.1 Отношения, связанные с возникновением, исполнением (осуществлением) и прекращением гражданских и иных прав и обязанностей, а также связанные с исполнением (осуществлением) и прекращением обязательств (обязанностей), возникших по основаниям, предусмотренных законом и иными нормативными правовыми актами.

Наименование организации:_____
_____
_____

Адрес места нахождения юридического лица:_____

Почтовый адрес юридического лица:_____

Ознакомлен(а) и настоящим заявляю о добровольном принятии мною, как должностным лицом Организации, Правил корпоративного ЭДО “Личный кабинет. Для клиентов инфраструктуры”, утвержденных ЗАО “Первый Специализированный Депозитарий”, и регламентирующих отношения, которые указаны в политике применения сертификата ключа подписи. Выражаю согласие с тем, что используемая техническая реализация электронного документооборота достаточна для обеспечения защиты информации от несанкционированного доступа, подтверждения подлинности, авторства электронных документов и разбора конфликтных ситуаций по ним, а также с тем, что документ, подписанный электронной цифровой подписью, которая соответствует данному сертификату ключа подписи, юридически эквивалентен документу на бумажном носителе, заверенному собственноручной подписью и печатью Организации.

Подписанием настоящего Заявления заявитель присоединяется к Регламенту изготовления и обслуживания сертификатов открытых ключей Удостоверяющего центра EKEY.ru, утвержденного ЗАО «Удостоверяющий центр», принимает и обязуется исполнять все содержащиеся в нем требования, правила и условия.

Согласен(а) с тем, что мои персональные данные могут обрабатываться, включая публикацию сертификата ключа подписи ЭЦП, содержащего мои персональные данные, в сети Интернет.

Лицо, запрашивающее сертификат _____/_____
(расшифровка подписи)
"___" _____ 200__г.

Ознакомлен(а) и настоящим заявляю о добровольном принятии Организацией Правил корпоративного ЭДО “Личный кабинет. Для клиентов инфраструктуры”, утвержденных ЗАО “Первый Специализированный Депозитарий”, и регламентирующих отношения, которые указаны в политике применения сертификата ключа подписи. Выражаю согласие с тем, что используемая техническая реализация электронного документооборота достаточна для обеспечения защиты информации от несанкционированного доступа, подтверждения подлинности, авторства электронных документов и разбора конфликтных ситуаций по ним, а также с тем, что документ, подписанный электронной цифровой подписью, которая соответствует данному сертификату ключа подписи, юридически эквивалентен документу на бумажном носителе, заверенному собственноручной подписью и печатью Организации.

Подписанием настоящего Заявления заявитель присоединяется к Регламенту изготовления и обслуживания сертификатов открытых ключей Удостоверяющего центра EKEY.ru, утвержденного ЗАО «Удостоверяющий центр», принимает и обязуется исполнять все содержащиеся в нем требования, правила и условия.

Данные о сотруднике, запрашивающем сертификат, его полномочиях, данные о наименовании, местонахождении и реквизитах Организации, указанных в заявлении, подтверждаю.

**Руководитель организации** _____/_____
(расшифровка подписи)

Приложение 4

Пример формы заявления на отзыв сертификата

**Генеральному директору**
**ЗАО "Удостоверяющий центр"**

_____

От: _____

Паспорт: _____

_____

_____

# ЗАЯВЛЕНИЕ
## на отзыв сертификата ключа ЭЦП

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

Серийный номер: _____

Общее имя: _____

Организация: _____

в связи с _____

_____/_____

"___" _____ 200__г.

М.П.

Прошито и
пронумеровано
6 (шесть) лист(ов)