Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

# Инструкция
# по обновлению сертификатов ключей подписи пользователей Удостоверяющего центра InfoTrust


Ижевск 2007

# Содержание

# 1 Общие положения

Настоящая инструкция предназначена для пользователей Удостоверяющего центра InfoTrust. Изготовление сертификатов ключей подписи производится в соответствии с Регламентом Удостоверяющего центра InfoTrust ООО Научно-производственное предприятие «Ижинформпроект».

Изготовление сертификата ключа подписи Пользователя УЦ осуществляется ежегодно при плановой, а также при внеплановой замене закрытого ключа подписи Пользователя УЦ.

В соответствии с требованиями Федерального закона от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи», руководствуясь инструкцией, пользователь УЦ сможет произвести самостоятельное формирование новых ключевых документов, направить запрос на сертификат ключа подписи в Удостоверяющий центр, получить и установить новый сертификат в своей операционной системе.

Формирование сертификата ключа подписи Пользователя УЦ осуществляется Удостоверяющим центром на основании Заявления об изготовлении сертификата ключа подписи Пользователя УЦ по установленной форме.

В том случае, если Пользователь УЦ не может прибыть лично в офис Удостоверяющего центра, Абонент Системы должен выдать лицу, пребывающему в офис Удостоверяющего центра, Доверенность на изготовление сертификата ключа подписи соответствующего Пользователя УЦ по установленной форме.

Ответственный сотрудник Удостоверяющего центра выполняет процедуру идентификации Пользователя УЦ или доверенного лица путем установления личности по паспорту.

После положительной идентификации Пользователя УЦ или доверенного лица Ответственный сотрудник Удостоверяющего центра принимает документы и осуществляет их рассмотрение.

При принятии положительного решения, Удостоверяющий центр изготавливает сертификат ключа подписи. Указанные действия выполняются Удостоверяющим центром в течение 3 (Трех) рабочих дней.

Пользователю УЦ предлагается поручить сформировать закрытые ключи Удостоверяющему центру или выполнить эту процедуру самостоятельно на своем рабочем месте с использованием программного обеспечения, предоставляемого Удостоверяющим центром.

Удостоверяющий центр InfoTrust гарантирует своевременное изготовление сертификата ключа подписи по данному запросу только при условии его представления (на бумаге и в электронном виде) не позднее, чем за 3 рабочих дня до планируемой даты выпуска, при условии оплаты услуг.

# 2 Генерация ключей Удостоверяющим центром

В случае генерации ключей Удостоверяющим центром Пользователь заполняет Заявление об изготовлении сертификата ключа пользователя по установленной форме. Для удобства может быть использована форма MS Word. При этом необходимо указать требуемый профиль сертификата.

На основании Заявления по окончании процедуры для Пользователя УЦ формируются:

— ключевой носитель, содержащий ключевой контейнер с закрытым ключом подписи, записанный в формате, определяемом средством электронной цифровой подписи;

— сертификат ключа подписи в электронной форме, соответствующий закрытому ключу;

— сертификат ключа подписи в виде документа на бумажном носителе;

— сертификат ключа подписи уполномоченного лица Удостоверяющего Центра в электронной форме.

Указанные выше данные, передаваемые зарегистрированному Пользователю УЦ в электронной форме (кроме ключей), записываются в виде файлов на магнитный диск 3,5”.

Документы на электронных и бумажных носителях выдаются/направляются Пользователю УЦ с соблюдением требований по обеспечению конфиденциальности.

До истечения 10-ти календарных дней с момента направления Пользователю УЦ документов на электронных и бумажных носителях Пользователь УЦ должен подписать два экземпляра сертификата ключа подписи в виде документа на бумажном носителе и предоставить Удостоверяющему центру один экземпляр.

# 3 Генерация ключей Пользователем УЦ

В случае генерации ключей Пользователем УЦ Пользователь заполняет Заявление об изготовлении сертификата ключа пользователя по установленной форме (Приложение А). Для удобства может быть использована форма MS Word. При этом необходимо указать требуемый профиль сертификата.

К Заявлению прилагается в бумажном и электронном виде соответствующий Запрос на сертификат, формируемый в процессе генерации ключей с использованием программного обеспечения (утилита), предоставляемого УЦ.

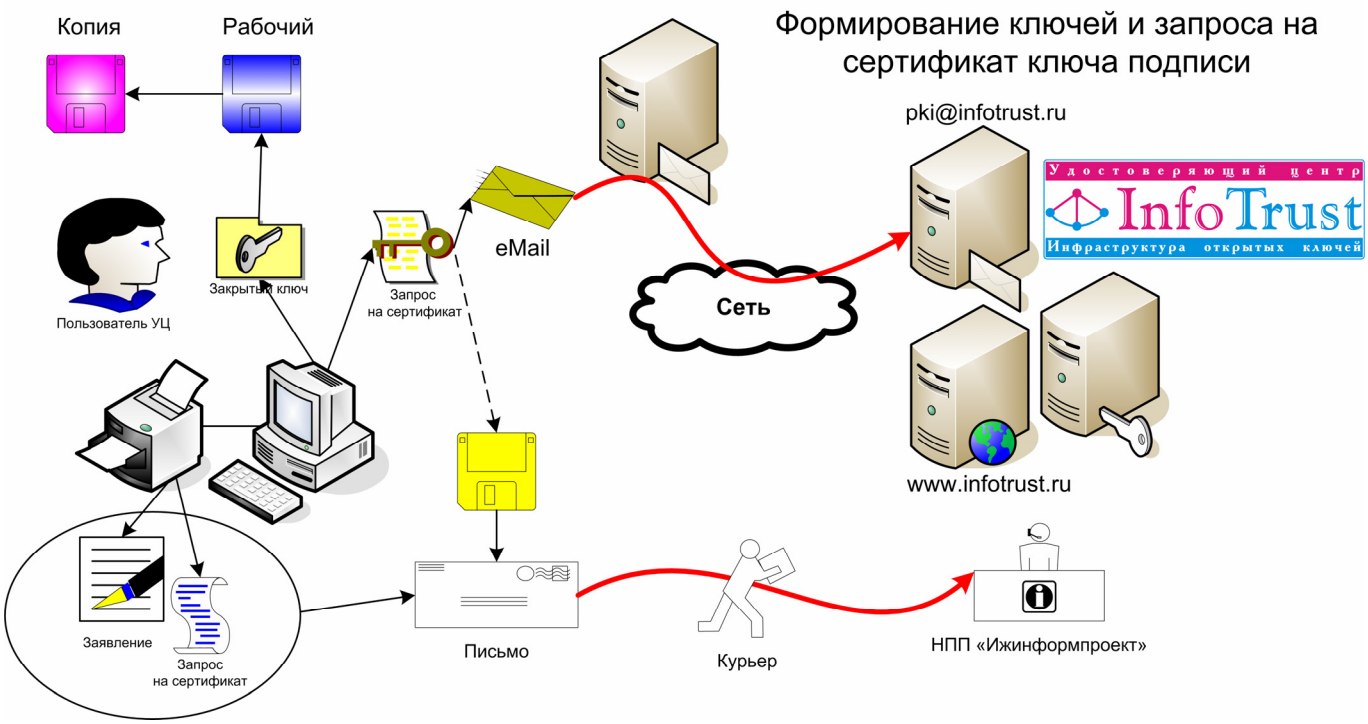

Сформированный запрос на сертификат в электронном виде необходимо направить по электронной почте на адрес pki@infotrust.ru (с контролем доставки) или записать на магнитный носитель 3,5" и приложить его к Заявлению (обязательно проверить исправность дискеты).

После регистрации полученного Заявления в Удостоверяющем центре ответственный сотрудник Удостоверяющего центра проверяет соответствие Заявления и Запроса, устанавливает его автора, затем сравнивает значения полей, содержащиеся в запросе на сертификат (в бумажном и электронном виде), со значениями, указанными в Заявлении автора запроса.

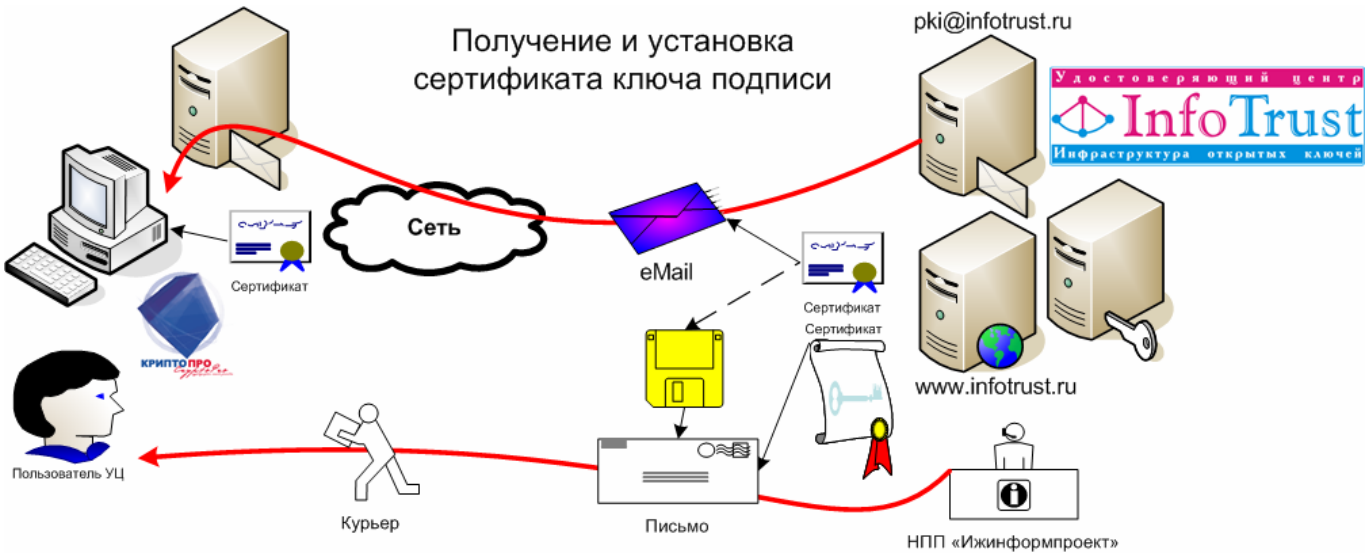
В случае положительного результата проведенных проверок по окончании процедуры для Пользователя УЦ формируются:

— сертификат ключа подписи в электронной форме, соответствующий закрытому ключу;

— сертификат ключа подписи в виде документа на бумажном носителе.




Сертификат ключа подписи в электронной форме направляется на адрес электронной почты, с которого поступил запрос пользователя, или записывается в виде файла на магнитный диск 3,5” пользователя.




До истечения 10-ти календарных дней с момента направления Пользователю УЦ документов на электронных и бумажных носителях Пользователь УЦ должен подписать два экземпляра сертификата ключа подписи в виде документа на бумажном носителе и предоставить Удостоверяющему центру один экземпляр.

# 4 Формирование запроса на сертификат ключа подписи

Прежде, чем начинать работу, убедитесь, что компьютер удовлетворяет следующим требованиям:

— MS Windows 2000/2003 и MS Windows XP SP2 (рекомендуется);

— СКЗИ КриптоПро CSP 2.0 или 3.0 (с установленными драйверами для поддержки используемых ключевых носителей);

— Internet Explorer 6.0.

— Доступ к принтеру для печати запроса на сертификат ключа подписи.

Для работы пользователю необходимо иметь:

— Установленный сертификат ключа подписи уполномоченного лица Удостоверяющего центра InfoTrust;

— Установленный сертификат ключа подписи зарегистрированного Пользователя, выданный Удостоверяющим центром InfoTrust, который планируется обновить.

**1** Подготовить (проверить работоспособность) новый ключевой носитель для формирования ключевых документов, а также носитель для резервной копии. Зарегистрировать указанные ключевые носители в соответствии с требованиями поэкземплярного учета СКЗИ и промаркировать их соответствующим образом.

**2** Для формирования ключевых документов и запроса на сертификат ключа подписи используется утилита InfoTrustCertRequestLite.

Утилиту можно загрузить с официального сайта УЦ InfoTrust по следующей ссылке www.infotrust.ru\data\Soft\InfoTrustCertRequestLite.zip или получить по электронной почте, написав запрос на адрес pki@infotrust.ru.

Распаковать полученный zip-архив с утилитой в папку на компьютер пользователя, запустить файл InfoTrustCertRequestLite.hta (рисунок 1).

**3** Выбрать обновляемый сертификат. Для этого нажмите на кнопку (подчеркнутую надпись) Выбрать (рисунок 1). В результате будет выведен список установленных сертификатов пользователя с возможностью выбора обновляемого сертификата (рисунок 2).

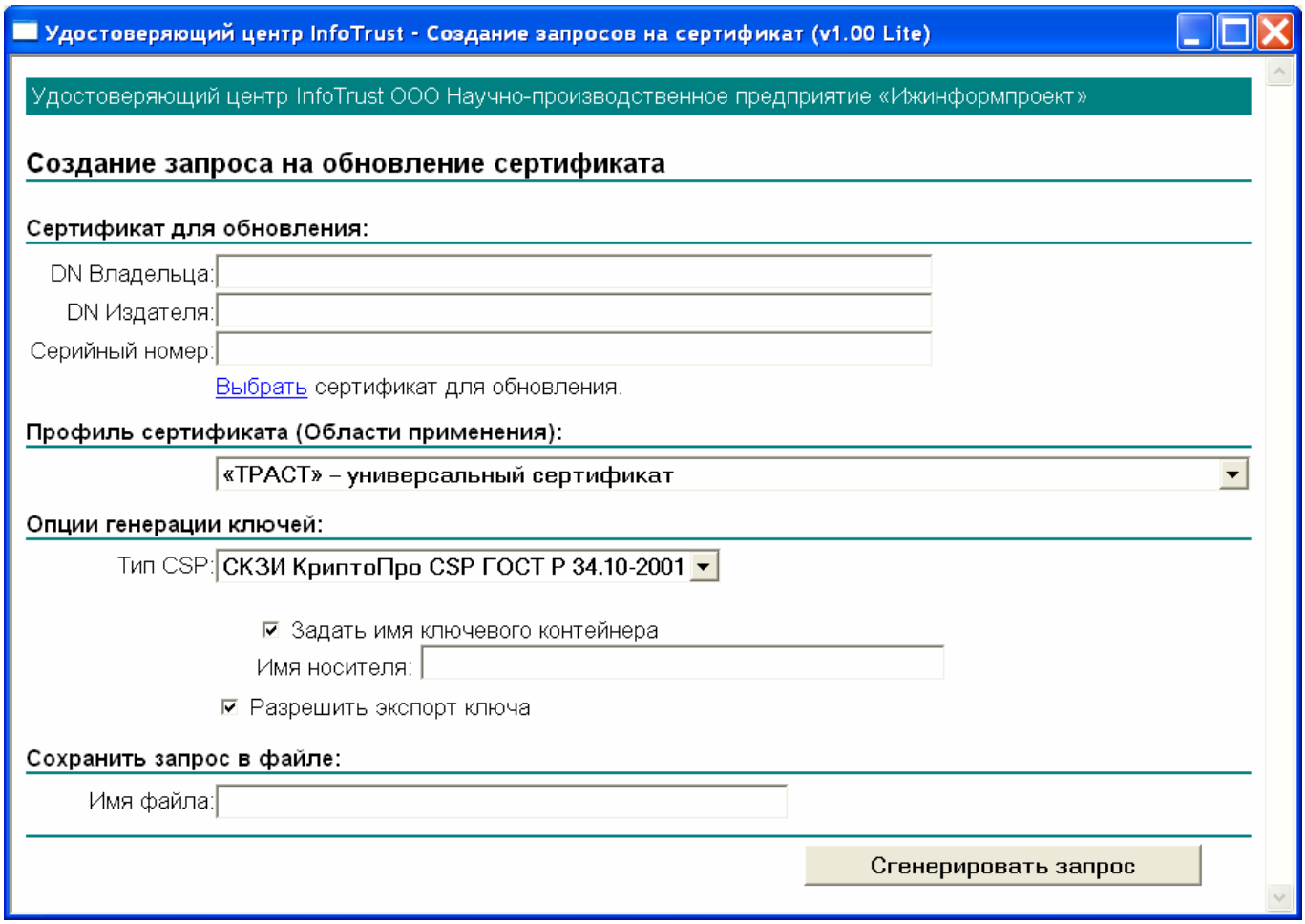



Рисунок 1 — Основное окно утилиты **InfoTrustCertRequestLite**

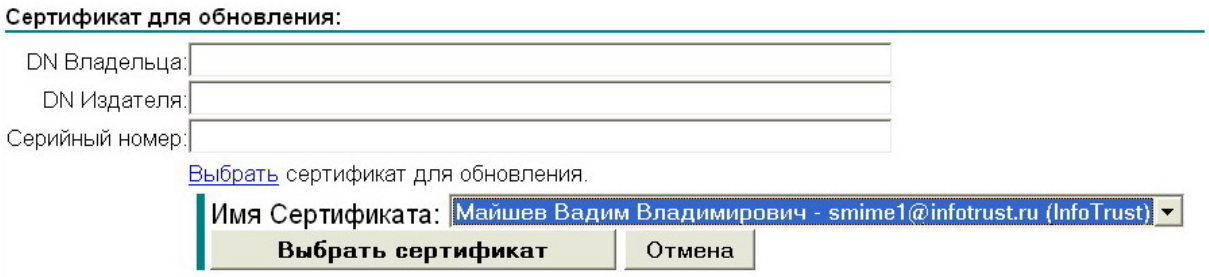



Рисунок 2 — Выбор сертификата

**4** Из предложенного списка необходимо отметить искомый сертификат и нажать на кнопку Выбрать сертификат. При этом необходимо проверить выбранный сертификат по соответствующим полям и серийному номеру (рисунок 3).

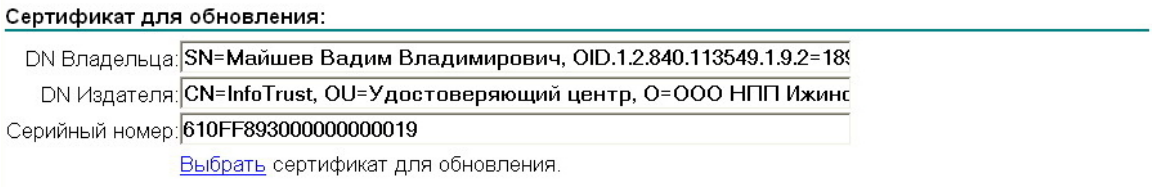



Рисунок 3 — Проверка выбранного сертификата

**5** Выбрать профиль сертификата (Области применения). Профиль сертификата выбирается исходя из используемой системы: «КриптоСвязь»{ОТЧЕТНОСТЬ через ИНТЕРНЕТ} — «ОТЧЕТ» или «ТРАСТ», «КриптоСвязь»{Защищенный Электронный Документооборот} — «ИНФРА», «УЛЬТРА» или «ТРАСТ» (рисунок 4).

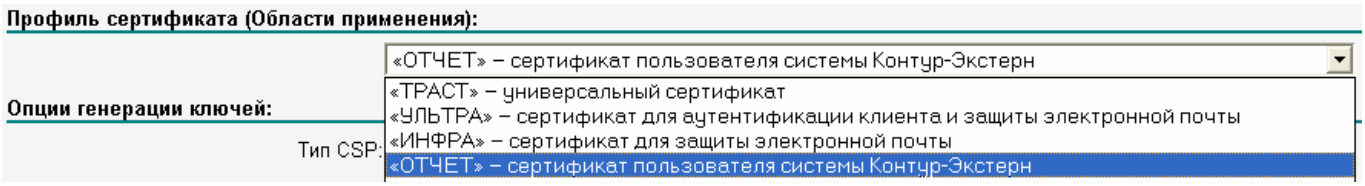



Рисунок 4 — Выбор профиля сертификата

**6** При необходимости задать имя контейнера закрытого ключа СКЗИ КриптоПро CSP. Рекомендуется оставить предлагаемое автоматически имя, которое формируется из поля CommonName сертификата и дополняется текущей датой. При повторной генерации ключей требуется задать новое имя. *Примечание: Длина поля «Имя носителя» не должна превышать 64 символа* (рисунок 5).

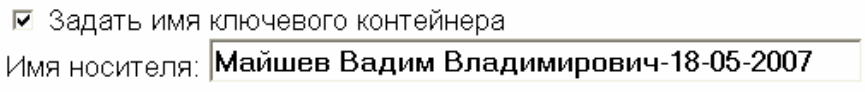



Рисунок 5 — Выбор имени ключевого контейнера

**7** Рекомендуется Разрешить экспорт ключа. Это позволит впоследствии копировать штатными средствами СКЗИ КриптоПро CSP создаваемый ключевой контейнер.

**8** Поле Имя файла указывает файл с расширением p10, который будет содержать запрос на сертификат. Рекомендуется оставить предлагаемое автоматически имя, которое формируется из поля CommonName сертификата. При повторной генерации ключей файл перезаписывается.

**9** Нажать кнопку Сгенерировать запрос (Рисунок 1).

**10** Выбрать среди установленных в СКЗИ КриптоПро CSP используемый носитель ключевой информации (Дискета/eToken/РУТОКЕН) (Рисунок 6).

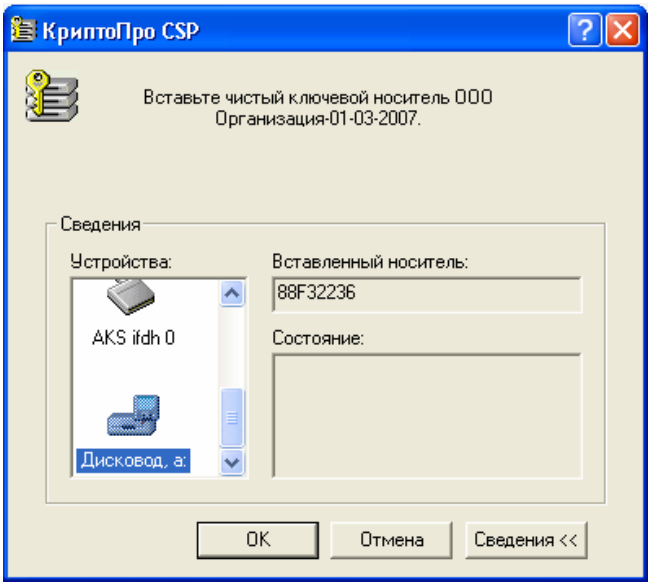



Рисунок 6 — Выбор ключевого носителя

**11** Если, при генерации запроса произошла ошибка, показанная на рисунке 7, то следует изменить имя носителя (см. рисунок 5) и попробовать снова.

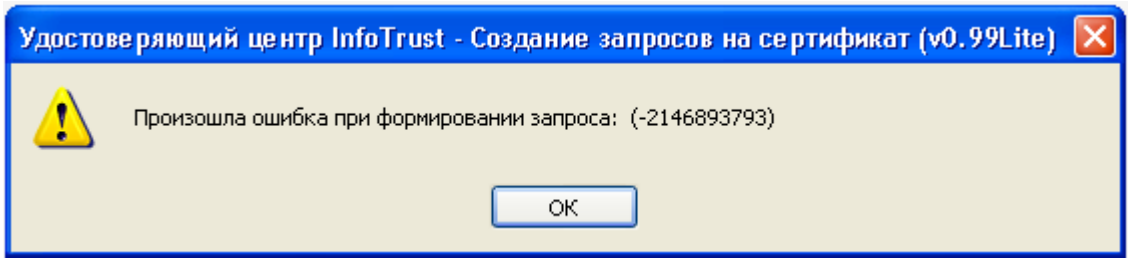



Рисунок 7 — Ошибка

**12** При формировании ключевой информации используется биологический датчик случайных чисел. Для этого требуется перемещать мышь или нажимать произвольные клавиши (рисунок 8).

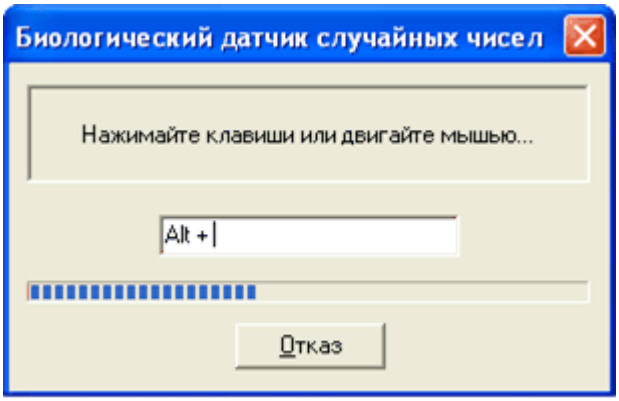



Рисунок 8 — Датчик случайных чисел

**13** При необходимости можно задать пароль для доступа к ключевому контейнеру. **ВНИМАНИЕ: в случае утраты пароля доступ к ключу будет**

**невозможен, что приведет к необходимости выпуска нового сертификата.** Для eToken/РУТОКЕН вводится действующий PIN пользователя (рисунок 9).

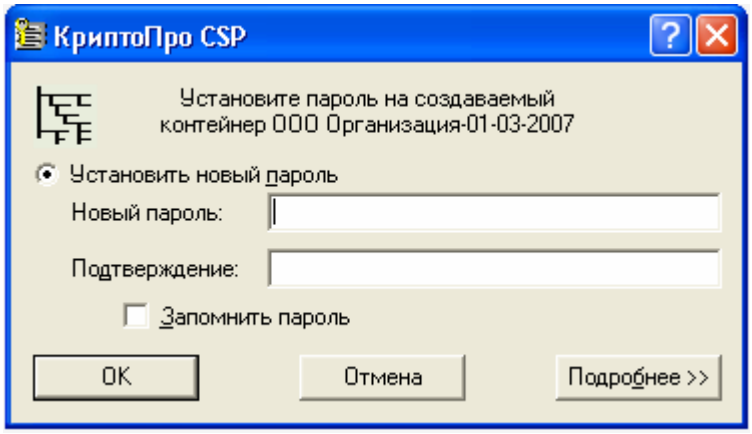



Рисунок 9 — Пароль для доступа к ключевому контейнеру

**14** После нажатия кнопки ОК (см. рисунок 9) отобразится «бумажная форма» (Приложение № 1 к Заявлению об изготовлении сертификата ключа подписи) сформированного запроса на сертификат ключа подписи (Приложение Б), которую необходимо распечатать. **ВНИМАНИЕ: форма не сохраняется.**

**15** В каталоге, из которого производился запуск утилиты **InfoTrustCertRequestLite,** будет создан файл с расширением p10, содержащий сформированный запрос на сертификат в электронном виде. Указанный файл не содержит конфиденциальной информации. Данный файл необходимо направить по электронной почте на адрес pki@infotrust.ru (с контролем доставки), указав в письме наименование организации, фамилию, имя, отчество пользователя и телефон для связи, или записать его на магнитный носитель 3,5" и приложить к Заявлению (обязательно проверить исправность дискеты).

**16** Во избежание утраты ключей произвести средствами СКЗИ КриптоПро CSP копирование созданного ключевого контейнера на носитель резервной копии: Пуск → Настройка → Панель управления → КриптоПро CSP → Сервис → Скопировать контейнер, выбрав при этом копируемый контейнер, задав имя новому контейнеру-копии и определив для него соответствующий носитель.

# 5 Порядок действий при получении нового сертификата ключа подписи

**1** Полученный сертификат ключа подписи необходимо установить (под учетной записью пользователя) средствами СКЗИ КриптоПро CSP в операционную систему:

Пуск → Настройка → Панель управления → КриптоПро CSP → Сервис → Установить личный сертификат, выбрав при установке файл с новым сертификатом ключа подписи и соответствующий ему ключевой контейнер, поместив его в хранилище Личные сертификаты.

**2** Настроить прикладные приложения (OutLook Express, КриптоАРМ и т.п.) для работы с новыми ключевыми документами и сертификатами ключей подписи.

**3** Произвести проверку работоспособности, а также при необходимости обмен сертификатами между корреспондентами.

# Приложение А. Заявление об изготовлении сертификата ключа подписи Пользователя УЦ InfoTrust

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
_____
_____

Паспорт: серия ☐☐ ☐☐ № ☐☐☐☐☐☐

Дата выдачи «___»_____ 200__

Выдан _____
_____

Телефон __(_____)_____

## Заявление об изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра InfoTrust

В связи с плановой / внеплановой (ненужное зачеркнуть) заменой ключевых документов прошу изготовить на мое имя сертификат ключа подписи с профилем «_____» для защищенной информационно-телекоммуникационной системы «КриптоСвязь».

В сертификате прошу указать сведения, предоставленные при моей регистрации в качестве Пользователя Удостоверяющего центра InfoTrust.

***Варианты для указания сертифицируемого ключа подписи — выбрать ☑ один из представленных:***

☐ Поручаю сформировать ключевые документы удостоверяющему центру.

☐ Сертификат изготовить на основании прилагаемого запроса в бумажном и электронном виде:

- ☐ — на магнитном диске 3,5”;
- ☐ — направлен на адрес электронной почты pki@infotrust.ru;

*В зависимости от сделанного выбора, изготовленный сертификат в электронном виде будет записан на магнитный диск 3,5” пользователя или направлен на адрес электронной почты, с которого поступил запрос.*

Примечание. Сертификат изготавливается удостоверяющим центром в течение трех рабочих дней с момента представления настоящего заявления с приложением (на бумаге и в электронном виде) при условии оплаты услуги.

Пользователь УЦ _____/_____/
«_____» _____ 200___

**Достоверность указанных сведений ПОДТВЕРЖДАЮ.**
Руководитель
_____ _____/_____/
м.п. «_____» _____ 200___

---

Личность заявителя установлена. «_____» _____ 200___

Сотрудник Удостоверяющего центра _____/_____/

# Приложение Б. Запрос на сертификат ключа подписи Пользователя УЦ InfoTrust

Приложение № 1 к Заявлению об изготовлении сертификата ключа подписи

## Удостоверяющий центр InfoTrust ООО Научно-производственное предприятие «Ижинформпроект»
## Запрос на сертификат ключа подписи

Прошу удостоверить факт принадлежности мне закрытого ключа электронной цифровой подписи, соответствующего указанному ниже открытому ключу электронной цифровой подписи, выпустив сертификат ключа подписи, указав в сертификате реквизиты, представленные при регистрации в качестве пользователя Удостоверяющего центра InfoTrust:

**Сведения о владельце ключа:**
**(CN) Имя сертификата:**
Майшев Вадим Владимирович
**Фамилия Имя Отчество:**
Майшев Вадим Владимирович
**Адрес e-mail:**
mvv@infotrust.ru
**ИНН-КПП-ИНН владельца** (обязательно для пользователей "КриптоСвязь"{Отчетность через Интернет}):
1899123456-189901001-189912345678
**Наименование организации:**
ООО НПП Ижинформпроект
**Город:**
Ижевск
**Регион:**
Удмуртская Республика
**Страна:**
RU

**Открытый ключ:**
**Алгоритм открытого ключа:**
**Название:** ГОСТ Р 34.10-2001
**Идентификатор:** 1.2.643.2.2.19
**Параметры:** 3012 0607 2A85 0302 0224 0006 072A 8503 0202 1E01
**Значение:** 0440 4D62 2E9C 41D8 259B C178 8A7B 0236 917A DD0E 41DE 1A52 9007 A82B F63D D09D 3F1C 8919 298F 35DC 39D8 1F1B 1F53 5865 5CCA 6658 4686 BAB5 FFE4 DCE3 8026 AE56 B6AE

Средство криптографической защиты информации "КриптоПро CSP"

«Подтверждаю действительность указанных выше сведений»

Пользователь Удостоверяющего центра InfoTrust: _____/Майшев Вадим Владимирович/
"___" _____ 2007 г.

Подписанный Запрос на сертификат ключа подписи следует приложить к Заявлению и доставить в Удостоверяющий центр InfoTrust по адресу:
ул. Бородина, 21, оф. 204, г. Ижевск, Удмуртская Республика, 426008

Сформированный запрос на сертификат в электронном виде необходимо направить по электронной почте на адрес pki@infotrust.ru (с контролем доставки) или записать на магнитный носитель 3,5" и приложить его к Заявлению (обязательно проверить исправность дискеты).
Внимание! Удостоверяющий центр InfoTrust гарантирует своевременное изготовление сертификата ключа подписи по данному запросу только при условии его представления (на бумаге и в электронном виде) не позднее, чем за 3 рабочих дня до планируемой даты выпуска.

«Заявитель является зарегистрированным пользователем Удостоверяющего центра InfoTrust.
Сведения об открытом ключе электронной цифровой подписи в запросе на сертификат, представленные в электронном виде и в настоящем документе совпадают»

Уполномоченный сотрудник Удостоверяющего центра InfoTrust: _____/_____/
"___" _____ 2007 г.