Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”
426057, г. Ижевск, ул. Бородина, 21, оф. 204. тел./факс 485-999, 48-55-88, www.infotrust.ru, info@infotrust.ru

Инструкция по использованию защищенного устройства хранения ключевой информации eToken в системе «КриптоСвязь»

Содержание

1 Общие сведения

Брелок или смарт-карта eToken имеет неоспоримые преимущества перед обычной дискетой, применяемой в качестве ключевого носителя.

Кроме того, eToken может работать с приложениями Microsoft Windows, а также может быть использован совместно с другими специальными средствами и системами защиты информации, например SecretDisk.

eToken — это смарт-карта или её полнофункциональный аналог, выполненный в виде USB-ключа. USB-ключ **eToken** напрямую подсоединяется к компьютеру через порт USB (Universal Serial Bus) и не требует наличия дорогостоящих считывателей или других дополнительных устройств.

eToken может иметь до 64 КБ защищённой энергонезависимой памяти (EEPROM). **eToken** используется в качестве портативного хранилища секретных данных (ключей шифрования, кодов доступа, паролей, учётных записей, сертификатов и пр.).

Для получения доступа к защищённым данным, хранящимся в памяти **eToken**, требуется ввести PIN-код (Personal Identification Number), являющийся аналогом пароля. PIN-код должен содержать минимум четыре символа. Для увеличения стойкости PIN-кода используйте последовательность из восьми или более символов, включающую буквы, цифры и специальные символы. Русские буквы и пробелы в PIN-код включать не рекомендуется. Для замены PIN-кода необходимо знание текущего PIN-кода.

Предустановленный PIN-код: 1234567890 (используется по умолчанию в новых ключах и смарт-картах).

ВНИМАНИЕ! Если пользователь забыл PIN-код, то применять eToken в дальнейшем он больше не сможет. Внимательно относитесь к хранению Вашего PIN-кода.

Модели eToken

При работе с **eToken** для хранения ключевой информации, предназначенной для средства криптографической защиты информации КриптоПро CSP 2.0, Вы можете использовать:

— USB-ключ **eToken R2**;

— USB-ключ **eToken Pro**.

eToken R2 имеет аппаратно реализованный алгоритм шифрования DESX с ключом 120 бит. Размер памяти: 8, 16, 32, 64 КБ.

В отличие от **eToken R2, eToken Pro** имеет чип смарт-карты, аппаратно реализующий алгоритмы RSA/1024, DES, TripleDES, SHA-1. **eToken Pro** снабжён встроенным генератором ключевых пар для асимметричного шифрования. При этом личные («закрытые») ключи никогда не покидают чип. В eToken Pro используется чип SLE66C Infineon, обеспечивающий высокий уровень безопасности (сертификат ITSEC LE4) и работающий с операционной системой Siemens CardOS/M4.

eToken Pro можно форматировать с помощью утилиты eToken Format, входящей в состав пакета eToken Utilities. При этом вся информация, хранящаяся в памяти eToken, стирается.

При форматировании **eToken Pro** также может быть задан пароль администратора. С помощью него, например, можно сменить забытый PIN-код.

Размер памяти: 16, 32, 64 КБ.

Преимущества использования eToken

Строгая аутентификация

eToken обеспечивает двухфакторную аутентификацию с использованием аппаратного ключа (смарт-карты) и PIN-кода. Двухфакторная аутентификация, для которой нужно знать нечто (PIN-код) и иметь нечто (eToken) намного надёжнее, чем использование имён пользователя и паролей, основанное лишь на знании этих имён пользователя и паролей.

Высокая защищённость

Секретная информация хранится в защищённой памяти ключа (смарт-карты).

PIN-код **eToken** защищён от подбора. При этом используется аппаратная задержка отклика, равная приблизительно одной секунде. Дополнительно для **eToken Pro** может быть установлено число возможных попыток неправильного ввода PIN-кода, при превышении которого **eToken** блокируется.

В целях безопасности пользователи могут периодически менять PIN-код своего **eToken**.

Воспользоваться потерянным или украденным **eToken** нельзя, т.к. для доступа к его памяти необходимо ввести PIN-код.

Имя eToken

Каждый **eToken** можно персонализировать, т.е. присвоить ему уникальное имя. Это позволит быстро определить хозяина ключа или смарт-карты без знания PIN-кода.

Компактность и удобство

Смарт-карта **eToken Pro** — пластиковая карточка стандартного размера. Её удобно хранить в кармане или бумажнике.

USB-ключ **eToken** имеет небольшой размер и легко размещается на связке с ключами. Электронные ключи **eToken** выпускаются в герметичных цветных корпусах.

Каждый USB-ключ **eToken** снабжён световым индикатором режимов работы. Горящий световой индикатор свидетельствует о готовности **eToken** к работе. Мигание светового индикатора **eToken Pro** отображает процессы чтения памяти ключа и записи в эту память.

Уникальность

Каждый eToken имеет 32-битный уникальный номер (ID).

Одновременное подключение

Возможна одновременная работа с несколькими **eToken** на одном компьютере.

2 Последовательность установки eToken

1 Подготовка системы к работе с USB-ключом eToken

2 Установка eToken RTE

3 Установка eToken для КриптоПро CSP 2.0

4 Добавление считывателей eToken в КриптоПро CSP

5 Настойка КриптоПро CSP

6 Копирование ключевого контейнера на eToken

7 Установка личного сертификата пользователя

3 Подготовка системы к работе с USB-ключом eToken

Внимание! eToken нельзя подключать до установки eToken RTE.

В случае если **eToken** подключен до установки eToken RTE, на экране появляются окна ***Поиск нового оборудования/Found New Hardware*** и ***Мастер обнаружения нового оборудования/Found New Hardware Wizard***.

При появлении этих окон на экране:

— в окне ***Мастер обнаружения нового оборудования/Found New Hardware Wizard*** нажмите ***Отмена/Cancel***;

— отключите eToken.

При добавлении новых портов USB может потребоваться переустановка eToken RTE.

При некорректной работе **eToken** проверьте настройки порта USB в BIOS. Для этого:

— перезагрузите компьютер, при перезагрузке откройте меню BIOS;

— убедитесь в том, что параметру ***Enable USB***, ***USB Controller***, ***USB Function*** и т. п. назначено значение ***Enable***, ***Enabled***, ***On*** и т.п.;

— убедитесь в том, что параметру ***Assign IRQ For USB***, ***Assign USB IRQ*** и т. п. назначено значение ***Enable***, ***Enabled***, ***On*** и т.п.

Для того чтобы убедиться в том, что поддержка USB-устройств включена в операционной системе Windows, выполните следующие действия.

1. Из ***Панели управления/Control Panel*** откройте ***Система/System***.

2. В окне ***Свойства системы/System Properties*** откройте вкладку ***Оборудование/Hardware***.

3. В Windows 2000/XP нажмите нажмите ***Диспетчер устройств/Device Manager***.

4. Убедитесь в том, что в дереве консоли присутствует узел ***Контроллеры универсальной последовательной шины USB/Universal Serial Bus Controllers***, а в нём - ***Корневой концентратор для USB/USB Root Hub***.

4 Установка eToken RTE

Для установки и удаления программного обеспечения требуются полномочия локального администратора.

Для того чтобы установить eToken Run Time Environment 3.00 (или более поздней версии), выполните следующую последовательность действий.

1. Запустить программу запуска или в меню компакт-диска нажмите ***Установить eToken RTE***. На экране появится окно приветствия программы установки eToken Run Time Environment 3.00.

2. В окне приветствия программы установки eToken Run Time Environment 3.00 нажмите ***Next***.

3. В окне ***eToken Run Time Environment 3.00 License Agreement*** ознакомьтесь с Лицензионным соглашением (на английском языке) и, если вы согласны с его условиями, выберите ***I accept the terms in the License Agreement (Я согласен/согласна с условиями Лицензионного соглашения)***, чтобы продолжить установку.

5. Отсоедините все **eToken** от компьютера.

6. В окне ***eToken Run Time Environment 3.00 Setup/Ready to Install*** нажмите ***Install***.

7. По завершении процесса установки eToken Run Time Environment 3.00 в окне ***eToken Run Time Environment 3.00 Setup/Completing the eToken Run Time Environment 3.00 Setup Wizard*** нажмите ***Finish***.

8. В случае необходимости возможно установить RUI — пользовательский интерфейс на русском языке (устанавливается после Run Time Environment).

Для проверки корректности настройки eToken RTE в операционной системе выполните следующие действия.

1. Убедитесь в том, что Ваш **eToken** подключен к компьютеру и его световой индикатор горит.

2. Из ***Панели управления/Control Panel*** откройте ***Система/System***.

3. В окне ***Свойства системы/System Properties*** откройте вкладку ***Оборудование/Hardware***.

4. В Windows 2000/XP нажмите ***Диспетчер устройств/Device Manager***.

5. Убедитесь в том, что в дереве консоли присутствует узел eToken, а в нём - один или более IFD Handler, а также один или более **eToken R2** или **eToken Pro**.

5 Установка eToken для КриптоПро CSP 2.0

Этот пункт в случае использования eToken Pro выполнять обязательно.

Для того чтобы установить eToken для КриптоПро CSP 2.0, выполните следующее.

1. Убедитесь в том, что на компьютере установлены eToken Run Time Environment 3.00 и КриптоПро CSP 2.0.

2. Запустите программу установки eToken для КриптоПро CSP 2.0.

3. В окне приветствия программы установки нажмите ***Далее***.

4. Ознакомьтесь с текстом лицензионного соглашения.

Если вы не согласны с условиями лицензионного соглашения, нажмите ***Отмена*** для прекращения установки. В этом случае eToken для КриптоПро CSP 2.0 не будет установлен.

Если вы согласны с условиями соглашения, выберите ***Я принимаю условия лицензионного соглашения*** и нажмите ***Далее***.

5. В окне eToken для КриптоПро CSP 2.0 - InstallShield Wizard/Готова к установке программы нажмите ***Установить***.

6. По окончании процесса установки в окне eToken для КриптоПро CSP 2.0 - InstallShield Wizard/Программа InstallShield Wizard завершена нажмите ***Готово***.

7. Перезагрузите компьютер.

6 Добавление считывателей eToken в КриптоПро CSP

Для того чтобы электронные USB-ключи **eToken R2** и **eToken Pro** и смарт-карты **eToken Pro** могли служить в качестве устройств хранения ключевой информации КриптоПро CSP 2.0, необходимо настроить КриптоПро CSP 2.0 на использование соответствующих считывателей. Настраивать считыватели могут только пользователи, наделённые полномочиями локального администратора.

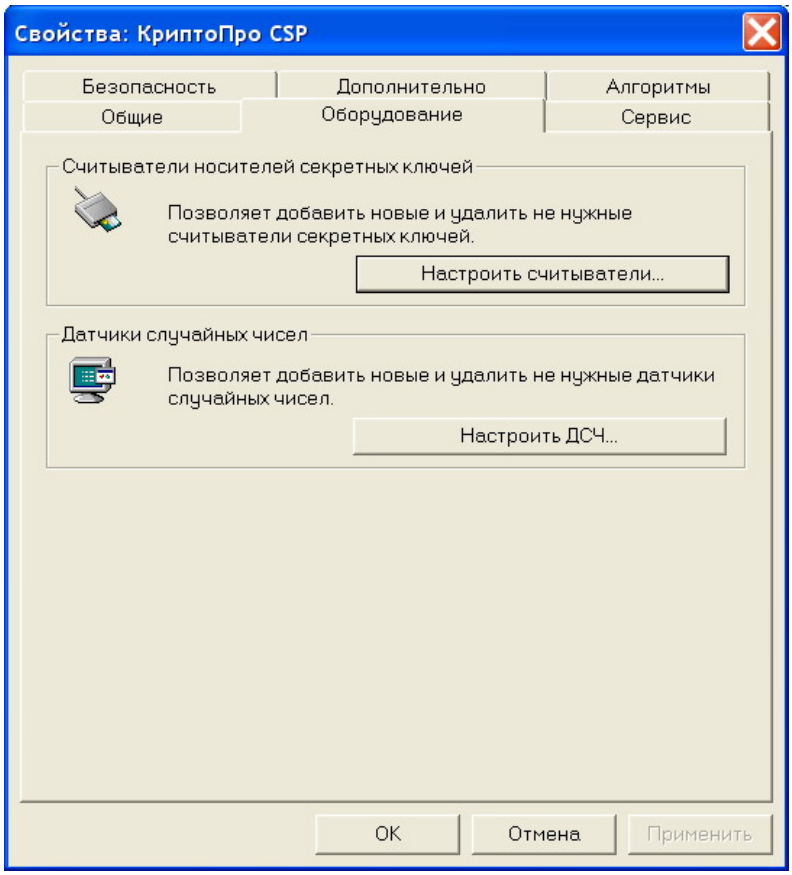
Для того чтобы настроить считыватели, выполните следующее.

1. Откройте ***Панель управления/Control Panel***.

2. Если вы используете в Windows XP вид панели управления по категориям (category view), выберите ***Прочие параметры панели управления/Other Control Panel Options***.

3. Выберите ***КриптоПро CSP/CryptoPro CSP***.

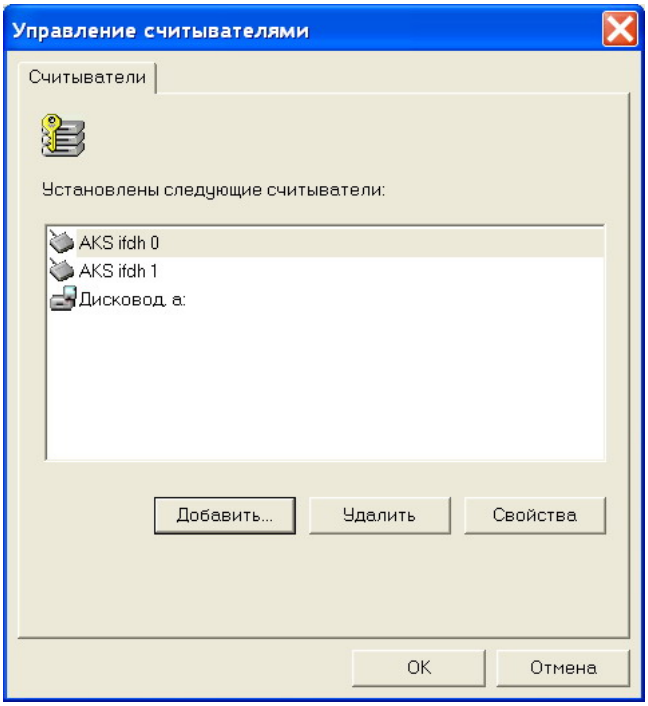
4. В окне ***Свойства: КриптоПро CSP/Properties: CryptoPro CSP*** выберите вкладку ***Оборудование/Hardware***.



5. Нажмите ***Настроить считыватели/Configure Carriers***.

6. В окне ***Управление считывателями/Readers' Control*** во вкладке ***Считыватели/Readers*** просмотрите список установленных считывателей.

7. Если вы хотите использовать USB-ключи **eToken**, КриптоПро CSP 2.0 должен быть настроен на использование логических устройств Aladdin IFD Handler (AKS ifdh) в качестве считывателей. Для использования смарт-карт **eToken Pro** необходимо, чтобы КриптоПро CSP использовал в качестве считывателя соответствующее устройство чтения смарт-карт. Если нужного устройства нет в списке, нажмите ***Добавить/Add*** для запуска мастера установки считывателя.



8. В первом окне мастера установки считывателя нажмите ***Далее/Next***.

9. В окне ***Мастер установки считывателя/Выбор считывателя (Reader Installation Wizard/Select Reader)*** выберите необходимое устройство и нажмите ***Далее/Next***.

10. В окне ***Мастер установки считывателя/Имя считывателя (Reader Installation Wizard/Reader Name)*** введите имя считывателя, если вы хотите заменить имя, назначенное мастером по умолчанию, и нажмите ***Далее/Next***.

11. В окне ***Мастер установки считывателя/Завершение работы мастера установки считывателя (Reader Installation Wizard/Reader Installation Completion)*** нажмите ***Готово/Finish***.

12. При необходимости добавьте ещё несколько считывателей. Если вы собираетесь использовать для хранения ключевой информации КриптоПро CSP 2.0 USB-ключи **eToken**, обязательно добавьте все имеющиеся в системе устройства Aladdin IFD Handler (AKS ifdh).

13. Убедитесь в том, что все необходимые считыватели установлены.

14. Установив все необходимые считыватели, в окне ***Управление считывателями/Readers' Control*** нажмите ***OK***.

15. В окне ***Свойства: КриптоПро CSP/Properties: CryptoPro CSP*** нажмите ***OK***.

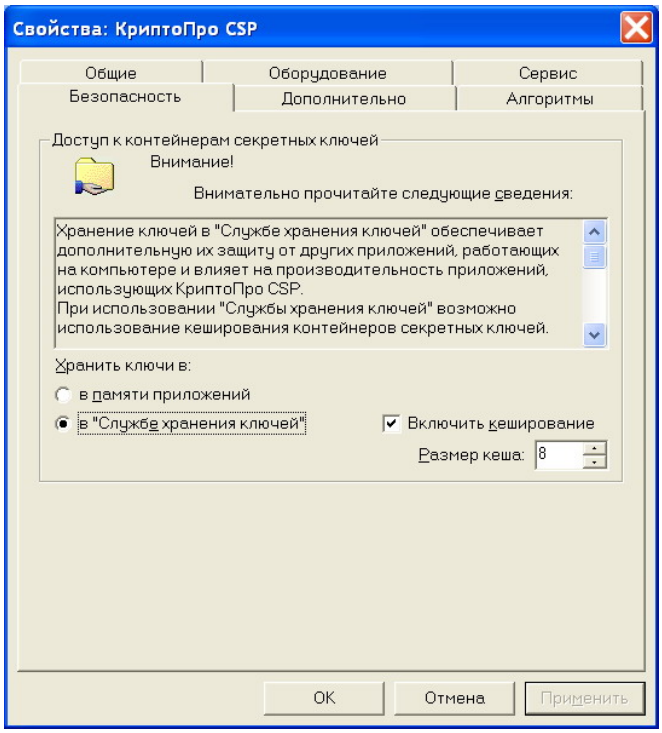
7 Настойка КриптоПро CSP

КриптоПро CSP может функционировать и хранить ключевую информацию в двух режимах:

— В памяти приложения.

— В «Службе хранения ключей», которая реализована в виде системного сервиса.

Функционирование КриптоПро CSP в «Службе хранения ключей» обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на компьютере, но может незначительно снизить производительность. Для изменения режима функционирования СКЗИ откройте панель настроек КриптоПро CSP как описано в предыдущем пункте и выберите необходимый режим.



Для повышения производительности рекомендуется включить кеширование.

8 Копирование ключевого контейнера на eToken

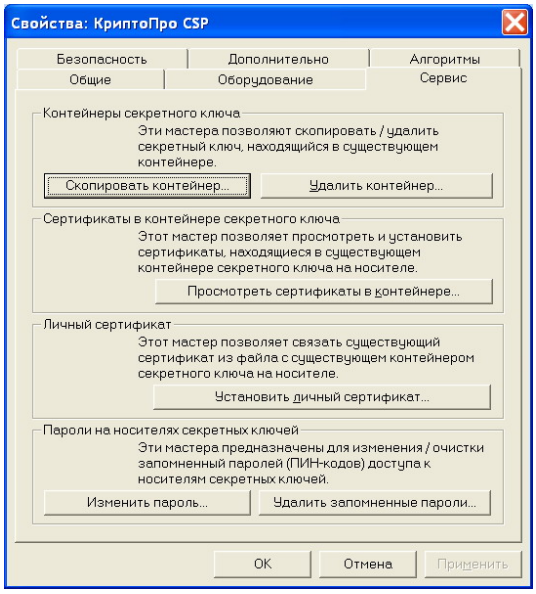
1. Откройте ***Панель управления/Control Panel***.

2. Если вы используете в Windows XP вид панели управления по категориям (category view), выберите ***Прочие параметры панели управления/Other Control Panel Options***.

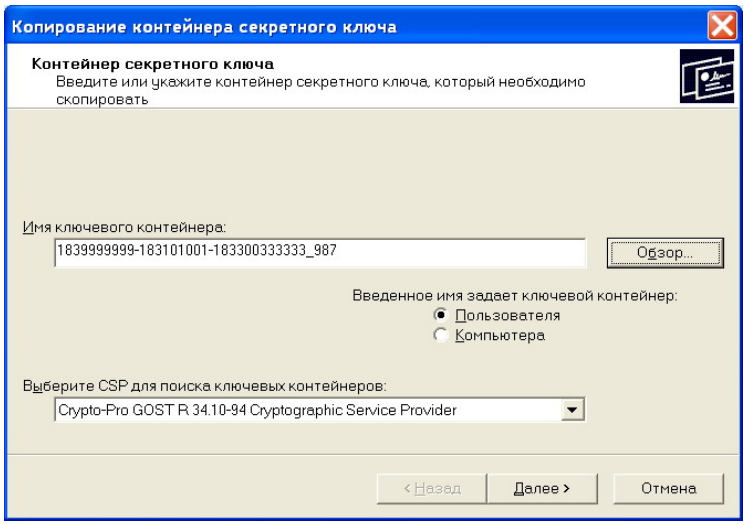
3. Выберите ***КриптоПро CSP/CryptoPro CSP***.

4. В окне ***Свойства: КриптоПро CSP/Properties: CryptoPro CSP*** выберите вкладку ***Сервис/Service***.

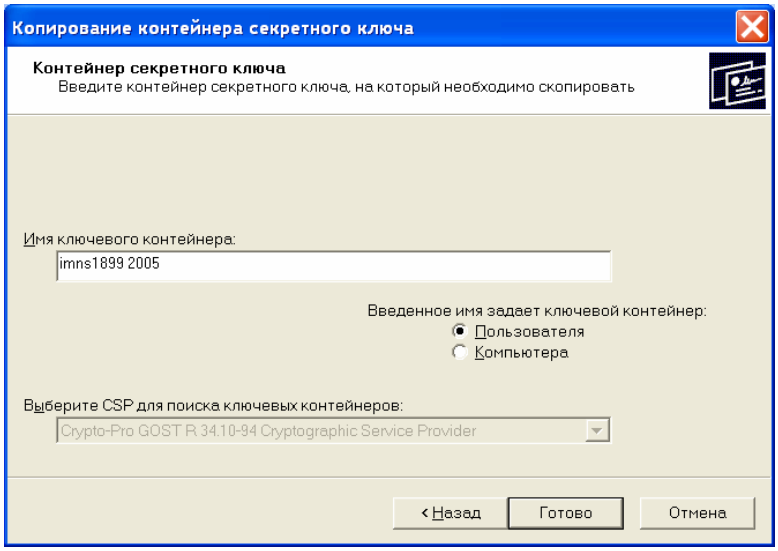
5. Нажмите ***Скопировать контейнер / Copy container***.



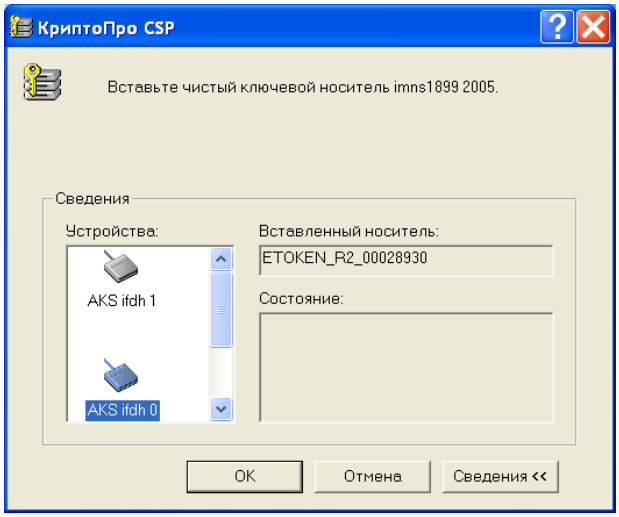
6. Вставить ключевую дискету в дисковод. Нажать ***Обзор / Browse,*** выбрать диск 3,5’’, выбрать на нем копируемый контейнер и нажать ***ОК***, ***Далее.***



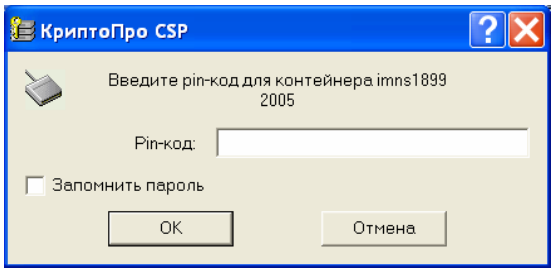
7. Ввести ***имя ключевого контейнера / key container name***, рекомендуется с указанием временных параметров (даты создания, периода действия и т.п.). Нажать ***Готово / Finish***.



8. Подключить и выбрать eToken



9. Ввести PIN-код для создаваемого контейнера — PIN-код **eToken**. Нажать ***OK***.



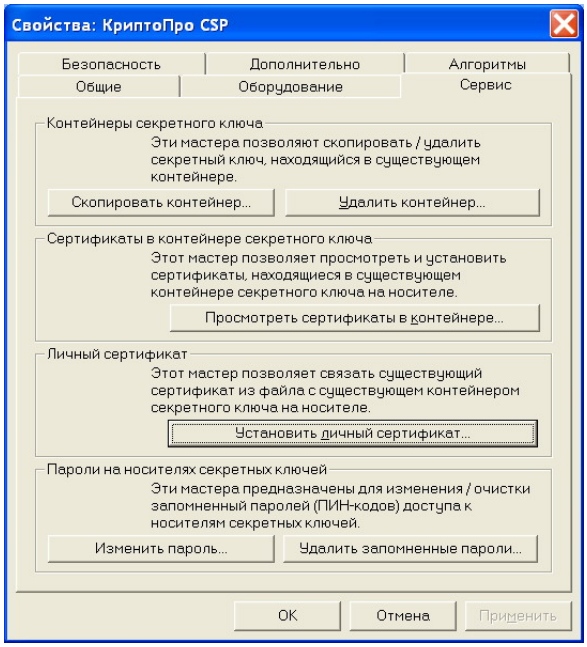
10. В окне ***Свойства: КриптоПро CSP/Properties: CryptoPro CSP*** нажмите ***OK***.

9 Установка личного сертификата пользователя

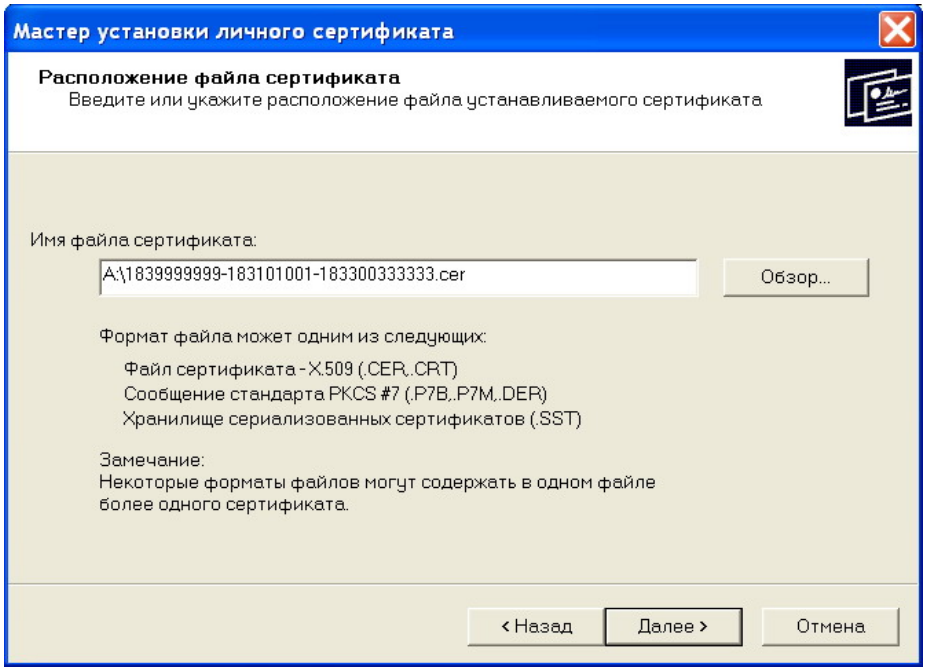
1. Откройте ***Панель управления/Control Panel***.

2. Если вы используете в Windows XP вид панели управления по категориям (category view), выберите ***Прочие параметры панели управления/Other Control Panel Options***.

3. Выберите ***КриптоПро CSP/CryptoPro CSP***.



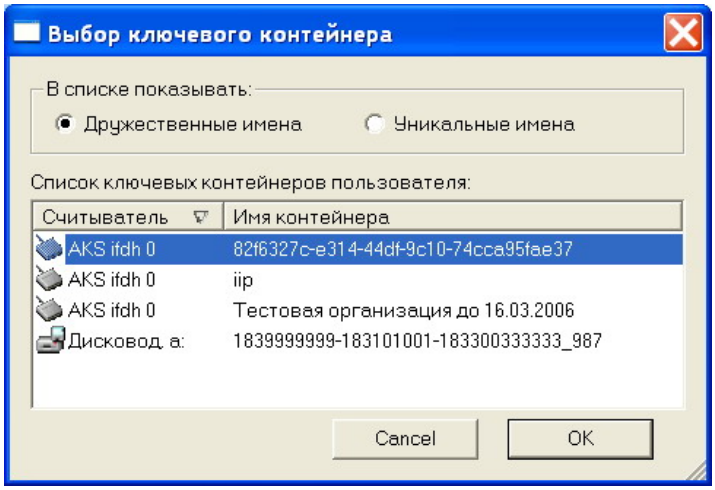
3. Во вкладке ***Сервис*** выбрать ***Установить личный сертификат***. В появившемся мастере нажать ***Далее***.



4. Нажать ***Обзор*** == > Выбрать файл сертификата

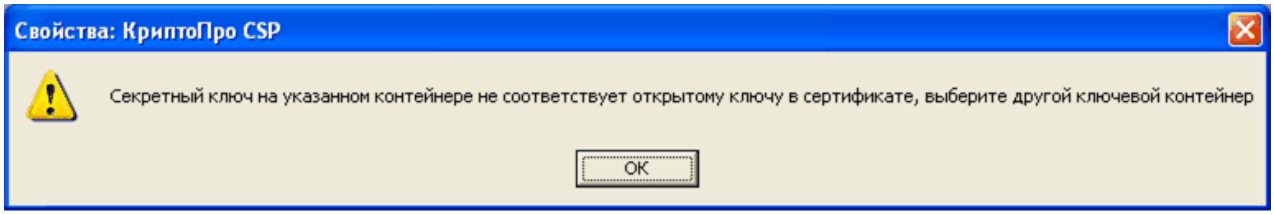
5. Нажать ***Далее*** == > В окне сведений о сертификате проверить что сертификат действительный (по датам) и нажать ***Свойства***.

6. Нажать ***Далее*** == > В окне выбора контейнера нажать ***Обзор***, выбрать соответствующий контейнер из eToken.



7. Нажать ***Далее*** == > Если вы выбрали правильный контейнер, появится ***Мастер установки личного сертификата.***

В случае, если выбор контейнера оказался неверным, появится следующее сообщение



8. Нажать ***Обзор*** == > В окне выбора хранилища сертификатов установить пункт ***Поместить все сертификаты в следующее хранилище***.

9. Нажать ***Обзор*** == > Выбрать папку ***Личные***, затем нажать ***ОК***, ***Далее***, ***Готово***.

10 Смена PIN-кода

Новые **eToken** имеют предустановленный на заводе PIN-код со значением 1234567890. В целях безопасности рекомендуется сменить PIN-код. Для этого:

1. Подключите **eToken**, PIN-код которого вы хотите сменить, к компьютеру. Световой индикатор USB-ключа **eToken** должен гореть.

2. Отключите все прочие **eToken**.

3. Щёлкните ***Пуск/Start*** > ***Все программы (Программы) / All Programs (Programs) > eToken > eToken Properties***.

4. В окне ***eToken Properties: Select an eToken*** щёлкните правой кнопкой мыши по строке с параметрами **eToken** в ячейке ***eToken Name***.

5. Выберите ***Change eToken Password***.

6. В появившемся окне введите текущий PIN-код в поле ***Current Password***, а новый PIN-код - в поля ***New Password*** и ***Confirm Password***.

Длина PIN-кода не может быть меньше 4 символов. Русские буквы и пробелы в PIN-коде использовать не рекомендуется. Для контроля за качеством нового PIN-кода вы можете нажать кнопку ***Show tips***. Если вы верно ввели PIN-код и подтверждение, станет доступной кнопка ***OK***.

7. Нажмите ***OK***.

8. В появившемся окне ***Change password*** нажмите ***OK***.

9. В окне ***eToken Properties: Select an eToken*** нажмите ***Exit***.

11 Переименование eToken

При выборе одного из подключенных к компьютеру **eToken** на экране выдается список, включающий имя **eToken**. Для того чтобы верно выбирать **eToken** из списка, рекомендуется присвоить каждому **eToken** уникальное имя. Для этого:

1. Подключите **eToken**, PIN-код которого вы хотите сменить, к компьютеру. Световой индикатор USB-ключа **eToken** должен гореть.

2. Отключите все прочие **eToken**.

3. Щёлкните ***Пуск/Start > Все программы (Программы) / All Programs (Programs) > eToken > eToken Properties***.

4. В окне ***eToken Properties: Select an eToken*** щёлкните правой кнопкой мыши по строке с параметрами **eToken** в ячейке ***eToken Name***.

5. Выберите ***Rename eToken***.

6. В появившемся окне введите PIN-код **eToken** и нажмите ***OK***.

7. Если ваш **eToken** имеет PIN-код по умолчанию (1234567890), может появиться окно с предупреждением и возможностью смены PIN-кода. Для того чтобы изменить PIN-код, введите новое значение дважды - в графы ***New Password*** и ***Confirm Password***. Длина PIN-кода не может быть меньше 4 символов. Русские буквы и пробелы в PIN-коде использовать не рекомендуется. Для контроля за качеством нового PIN-кода вы можете нажать кнопку ***Show tips***. Для сохранения нового PIN-кода нажмите ***OK***. Для того чтобы отказаться от смены PIN-кода, нажмите ***Cancel***.

8. Внесите изменения в поле ***eToken Name*** и нажмите ***Exit***.