Aladdin
SECURITY SOLUTIONS
www.aladdin.ru

eToken для КриптоПро CSP 3.6

Справочное руководство

Листов: 30

2010г.

Содержание

Лицензионное соглашение на использование программного обеспечения

Настоящее лицензионное соглашение (далее «Соглашение») является договором, заключенным между Вами (физическим или юридическим лицом) - конечным пользователем (далее «Пользователь») и компанией Aladdin Software Security R. D. (далее «Правообладатель») относительно передачи неисключительного права на использование программного обеспечения.

Программное обеспечение (далее «ПО») - это комплекс программ для ЭВМ, и документации (печатные материалы, носители и файлы с информацией), являющихся неотъемлемой частью ПО.

ПО, включая все дальнейшие усовершенствования, является объектом авторского права и охраняется законом.

1. Предмет Соглашения

Предметом настоящего Соглашения является передача Правообладателем конечному Пользователю неисключительного права на использование ПО.

Все условия, оговоренные далее, относятся как к ПО в целом, так и ко всем его компонентам в отдельности.

2. Имущественные права

Имущественные авторские права на данное ПО принадлежат исключительно Правообладателю.

Вам, конечному Пользователю, предоставляется неисключительное право на использование ПО в указанных в документации целях и при соблюдении приведенных ниже условий.

3. Условия использования

ПО может быть использовано только в строгом соответствии с документами, инструкциями и рекомендациями Правообладателя, относящимися к данному ПО.

Вы можете установить ПО как на одном, так и на нескольких компьютерах и использовать ПО одновременно без отчисления лицензионных платежей, при условии приобретения необходимого для работы количества персональных электронных ключей. Для работы с ПО одного Пользователя на одном рабочем месте необходим один персональный электронный ключ.

4. Обязательства

Вы обязуетесь не распространять ПО, т.е. не передавать его для последующего использования третьим лицам. Под распространением ПО понимается предоставление доступа третьим лицам к воспроизведенным в любой форме компонентам ПО, в том числе сетевыми и иными способами, а также путем их продажи, проката, сдачи внаем или предоставления взаймы.

Вы не имеете права осуществлять самостоятельно или разрешать другим лицам осуществлять следующую деятельность:

- допускать использование ПО людьми, не имеющими прав на использование данного ПО и работающими в одной сети или многопользовательской системе с Вами;

- пытаться дизассемблировать, декомпилировать (преобразовывать объектный код в исходный) программы, драйверы и другие компоненты ПО;

- вносить какие-либо изменения в код программ, драйверов или баз данных к ним, за исключением тех, которые вносятся штатными средствами, включенными в комплект поставки ПО и описанными в документации, а также разбирать и анализировать аппаратные средства, входящие в состав ПО, выяснять их устройство и принципы работы;

- предоставлять авторские права на использование программ или другие права на ПО третьим лицам;

- совершать относительно ПО другие действия, нарушающие российское законодательство и нормы международных договоров по авторскому праву, включая использование программных средств.

5. Срок действия Договора

Настоящий Договор вступает в силу с момента нажатия Вами кнопки «Далее» программы установки ПО и действует на протяжении всего срока использования ПО.

В случае нарушения Вами условий настоящего Соглашения или неспособности далее выполнять его условия, Вы обязуетесь уничтожить все копии ПО (включая архивные, файлы с информацией, носители, печатные материалы) или вернуть все относящиеся к ПО материалы организации, в которой Вы приобрели ПО. После этого Соглашение прекращает свое действие.

6. Ответственность

Нелегальное использование, распространение и воспроизведение (копирование) программного обеспечения является нарушением Закона РФ "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по Закону.

В случае нарушения настоящего Соглашения Правообладатель лишает Пользователя права на использование ПО. При этом Правообладатель полностью отказывается от своих гарантийных обязательств.

7. Гарантии

Правообладатель гарантирует соответствие компонентов ПО спецификациям, а также работоспособность ПО при выполнении Пользователем условий, оговоренных в документации на ПО.

ПО поставляется "таким, какое оно есть". Правообладатель не гарантирует, что ПО соответствует Вашим требованиям, и все действия ПО будут выполняться безошибочно.

Правообладатель не гарантирует корректную совместную работу ПО с программным обеспечением или оборудованием других производителей.

8. Отказ от ответственности за косвенный ущерб

В объеме, допускаемом действующим законодательством, Правообладатель не несет ответственность за какие-либо убытки (включая реальный ущерб и упущенную выгоду), возникшие из-за использования или невозможности использования ПО.

Я ПРОЧИТАЛ И ПОНЯЛ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ СО ВСЕМИ ОГОВОРЕННЫМИ В НЕМ ПУНКТАМИ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПО.

Общие сведения

Назначение

eToken для КриптоПро CSP 3.6 — модуль, позволяющий использовать USB-ключи и смарт-карты eToken в качестве устройств хранения ключевой информации КриптоПро CSP 3.6. При установленном eToken для КриптоПро CSP 3.6 операции с ключевой информацией КриптоПро CSP 3.6, хранящейся в памяти eToken, полностью аналогичны операциям с ключевой информацией КриптоПро CSP 3.6 на других устройствах.

.

Ключевые контейнеры

Ключевая информация КриптоПро CSP 3.6 – сертификаты и криптографические ключи – хранится в так называемых *ключевых контейнерах*.. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п.

«eToken для КриптоПро CSP 3.6» позволяет хранить ключевые контейнеры в защищенной памяти eToken, тем самым обеспечивая ряд дополнительных преимуществ.

Примечание

«eToken для КриптоПро CSP 3.6» версии 3.1 не поддерживает ключевые контейнеры, созданные с помощью «eToken для КриптоПро CSP 3.6» версии 1.x. Если в памяти вашего eToken есть такие контейнеры, вы не сможете их применять после установки «eToken для КриптоПро CSP 3.6» версии 3.1.

Преимущества

- **Безопасность ключевой информации**. Ключевая информация СКЗИ КриптоПро CSP (цифровые сертификаты, закрытые ключи ЭЦП и шифрования) хранится в защищённой ПИН-кодом памяти eToken, а не на диске компьютера. Сам eToken аппаратно защищён от перебора ПИН-кодов. Электронные ключи и смарт-карты eToken PRO соответствуют требованиями руководящего документа Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", сертифицированы по международному стандарту безопасности FIPS 140-1 (уровни 2 и 3), а используемая в них операционная система - по стандарту ITSEC Level E4.
- **Надёжность**. Ключевая информация СКЗИ КриптоПро CSP хранится в защищённой памяти eToken и остаётся в сохранности и безопасности даже в случае поломки компьютера или его утери.
- **Мобильность**. Малый размер USB-ключа eToken позволяет легко носить ключ с собой и всегда иметь возможность работы с защищённой почтой и удалённого защищённого доступа к корпоративным ресурсам и т.д. Смарт-карта eToken PRO имеет размер обычной кредитной карточки.
- **Соответствие стандартам**. eToken соответствует российским и международным стандартам качества и безопасности, а также совместим с ведущими продуктами мировых вендоров: IBM, Microsoft, Oracle и др. Сегодня eToken является стандартом "де-факто" на российском рынке USB-ключей / смарт-карт для информационной безопасности, позволяя хранить в памяти одного eToken цифровые сертификаты, ключи, пароли, коды доступа для более чем 200 различных приложений ведущих отечественных и мировых разработчиков ПО и средств ИБ.
- **Защита инвестиций**. В зависимости от сложившейся в организации IT-инфраструктуры можно выбрать оптимальный форм-фактор eToken: USB-ключ или смарт-карта.
- **Единое средство аутентификации и контроля доступа**. USB-ключи и смарт-карты eToken могут быть дополнены пассивными радиометками (RFID-метками) для использования их в системах контроля и управления доступом (СКУД). На поверхности смарт-карты eToken может быть напечатана фотография владельца для его визуальной идентификации.

Новое в версии

В версию 3.1 включена поддержка eToken PKI Client версии 5.1 SP1, что в первую очередь дает возможность использовать в качестве носителей электронные ключи и смарт-карты eToken на платформе Java.

Состав дистрибутива

Дистрибутив модуля поставляется двумя способами:

- в виде архива, который можно загрузить с сайта компании Aladdin.
- в составе дистрибутива программного продукта, использующего КриптоПро CSP 3.6.

На сайте Aladdin архив содержит:

- eToken_for_CryptoPro_x64.msp – пакет обновления для криптопровайдера КриптоПро CSP (для аппаратной платформы x64).
- eToken_for_CryptoPro_x86.msp – пакет обновления для криптопровайдера КриптоПро CSP (для аппаратной платформы x86).
- eTCPCSP3_6.pdf в папке RUS – краткое справочное руководство (этот файл).

Системные требования

Требования к программному обеспечению

Для работы eToken для КриптоПро CSP 3.0 необходим персональный компьютер со следующим программным обеспечением:

Для работы eToken для КриптоПро CSP 3.6 необходим персональный компьютер со следующим программным обеспечением:

1. Любая из операционных систем:

- Windows 2000 (IA32);
- Windows XP (IA32);
- Windows 2000 (IA32);
- Windows Server 2003 (IA32);
- Windows Server 2008 (IA32).

2. Microsoft Internet Explorer версии 5.0 или выше;

3. Любой из наборов драйверов eToken:

- eToken PKI Client 4.5 / 4.55 / 5.0 / 5.1 / 5.1 SP1: обязательно для устройств eToken на платформе eToken Java (см. таблицу ниже)
- eToken RTE 3.51 / 3.66;

4. Дополнительные драйверы для считывателей смарт-карт, если такие используются;

- КриптоПро CSP версии 3.6.

Требования к аппаратному обеспечению

Для работы eToken для КриптоПро CSP 3.0 необходим персональный компьютер со свободным портом USB для USB-ключей eToken и/или считывателем смарт-карт – для смарт-карт eToken PRO.

Для успешной работы eToken для КриптоПро CSP 3.0 необходимо, чтобы максимальный свободный блок в памяти eToken имел размер не менее 2 КБ.

USB-ключ или смарт-карта eToken:

- eToken GT;
- eToken NG-FLASH (Java);
- eToken NG-FLASH с операционной системой Siemens CardOS V4.2b;
- eToken NG-OTP (Java);
- eToken NG-OTP с операционной системой Siemens CardOS V4.2b;
- eToken PRO (Java);
- eToken PRO с операционной системой Siemens CardOS V4.2b.

Таблица совместимости программных и аппаратных компонентов

Операционная система	Набор драйверов	Модели eToken
Windows 2000 (IA32) Windows 2000 Server (IA32) Windows XP (IA32)	eToken RTE 3.51 / 3.66 eToken RTE 3.51 / 3.66 eToken RTE 3.51 / 3.66	• eToken NG-FLASH с операционной системой Siemens CardOS V4.2b; • eToken NG-OTP с операционной системой Siemens CardOS V4.2b; • eToken PRO с операционной системой Siemens CardOS V4.2b.
	eToken PKI Client 4.5 (или более новой версии)	• eToken GT; • eToken NG-FLASH (Java); • eToken NG-FLASH с операционной системой Siemens CardOS V4.2b; • eToken NG-OTP (Java); • eToken NG-OTP с операционной системой Siemens CardOS V4.2b; • eToken PRO (Java); • eToken PRO с операционной системой Siemens CardOS V4.2b.
Windows 2003 Server (IA32) Windows Server 2008 (IA32/x64) Windows Vista (IA32/x64)	eToken RTE 3.51 / 3.66	• eToken NG-FLASH с операционной системой Siemens CardOS V4.2b; • eToken NG-OTP с операционной системой Siemens CardOS V4.2b; • eToken PRO с операционной системой Siemens CardOS V4.2b.
	eToken PKI Client 4.5 (или более новой версии)	• eToken GT; • eToken NG-FLASH (Java); • eToken NG-FLASH с операционной системой Siemens CardOS V4.2b; • eToken NG-OTP (Java); • eToken NG-OTP с операционной системой Siemens CardOS V4.2b; • eToken PRO (Java); • eToken PRO с операционной системой Siemens CardOS V4.2b.

Установка

Модуль eToken для КриптоПро CSP 3.6 устанавливается как обновление для уже установленного модуля поддержки eToken для КриптоПро CSP 3.6.

В первую очередь необходимо настроить eToken для КриптоПро CSP 3.6 на работу со считывателями, которые будут использоваться для подключения устройств eToken.

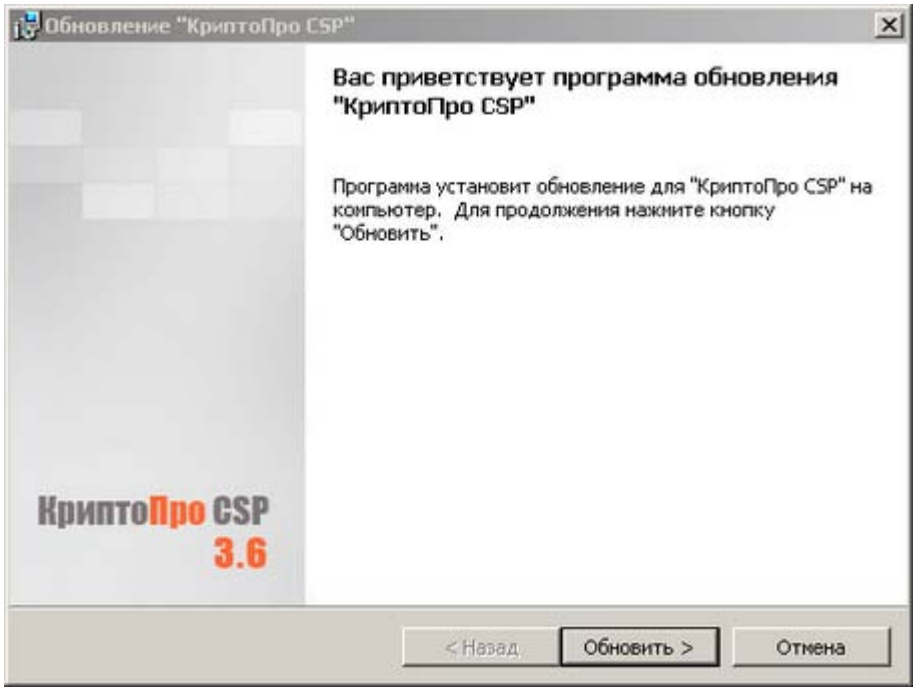
Вторым этапом, вам необходимо будет добавить носители – те модели eToken, которые вы будете использовать для хранения ключевых контейнеров.

Примечание

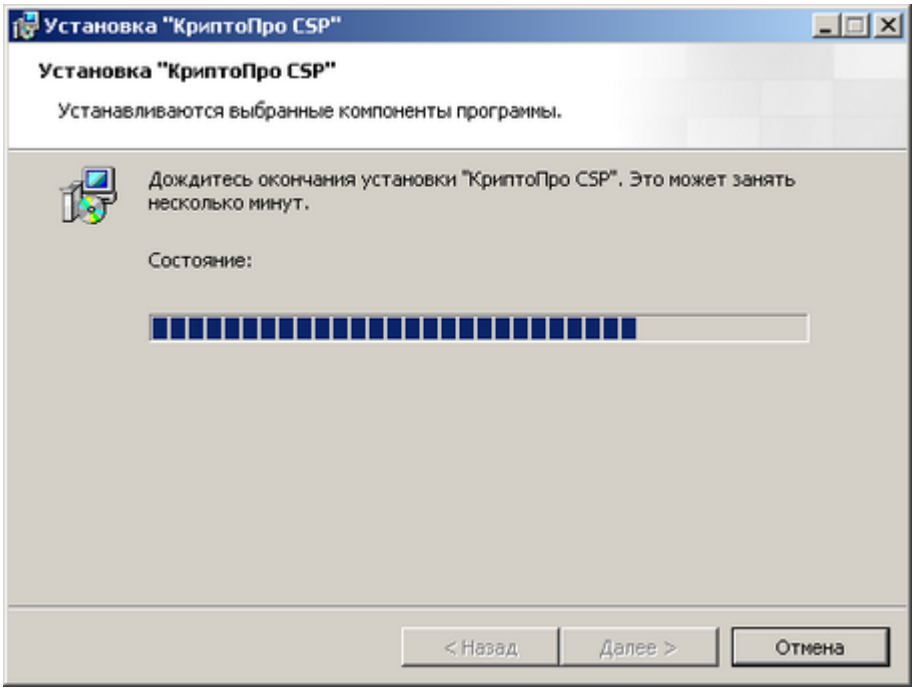
Для установки и удаления программного обеспечения требуются полномочия локального администратора.

Весь процесс установки выполняется с помощью программы-мастера. При этом будет добавлена библиотеки поддержки eToken и необходимые параметры реестра. Чтобы установить модуль eToken для КриптоПро CSP 3.6 выполните следующие действия:

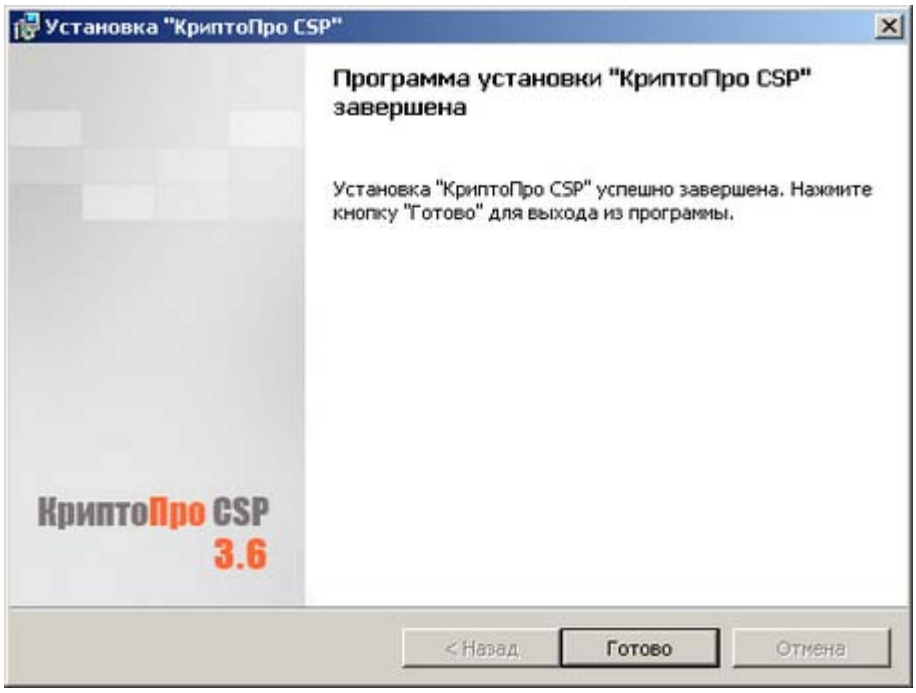
1. В зависимости от используемой операционной системы запустите eToken_for_CryptoPro_x64.msp или eToken_for_CryptoPro_x86.msp.
2. В окне программы-мастера нажмите кнопку **Обновить**.



После этого сразу начнется процесс установки модуля поддержки и настройки параметров реестра. Текущее состояние процесса отображается в виде шкалы с комментариями по каждому этапу.



3. После завершения установки на экране появится новое окно с соответствующим сообщением. Закройте его, нажав кнопку **Готово**.



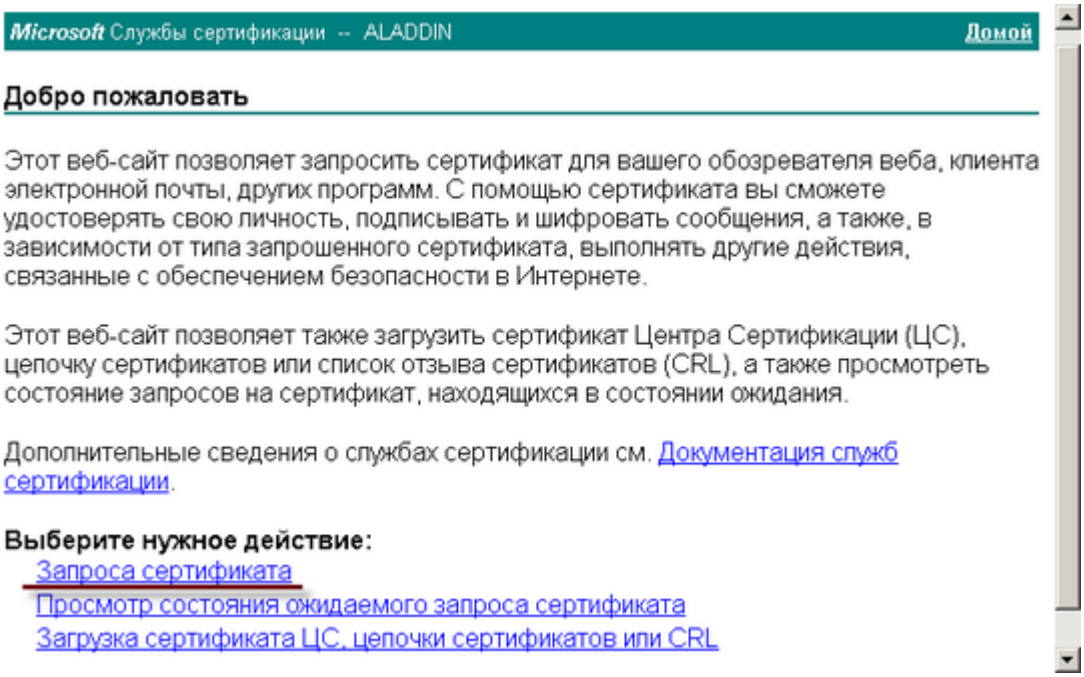
Работа с модулем eToken для КриптоПро CSP 3.6

Запись сертификатов в память eToken

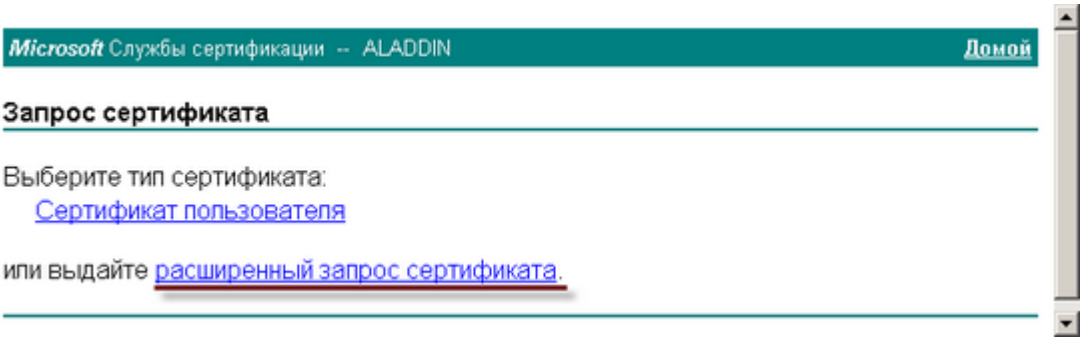
Процедура запроса на получение сертификата и записи полученного сертификата в память eToken при работе с КриптоПро CSP 3.6 аналогична обычному порядку получения сертификатов средствами Windows и КриптоПро CSP.

Например, для генерирования ключевой пары и получения сертификата на веб-узле центра сертификации предприятия на основе Windows Server 2003 выполните следующую последовательность действий:

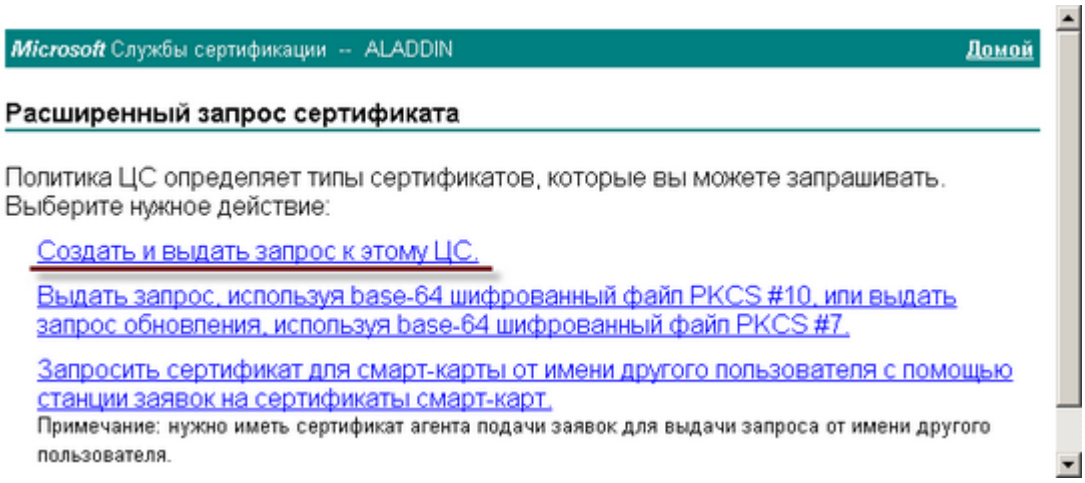
1. На домашней странице веб-узла службы сертификации выберите пункт, выделенный на картинке внизу, и нажмите **Далее**.



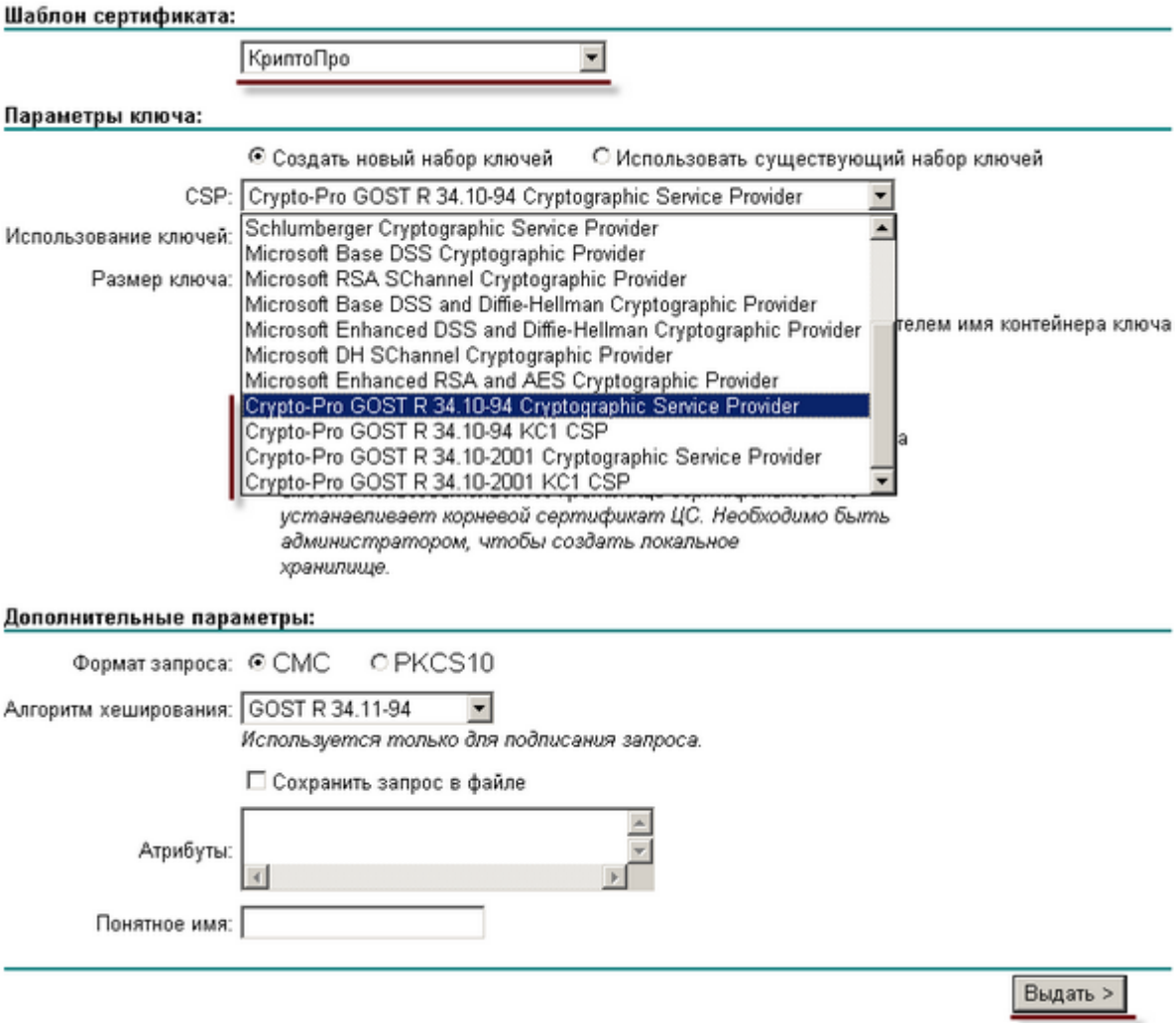
3. На странице выбора типа запроса выберите **Расширенный запрос** и нажмите **Далее**.



4. На странице **Расширенный запросы сертификата щелкните на ссылке Создать и выдать запрос к этому ЦС** и нажмите **Далее**.

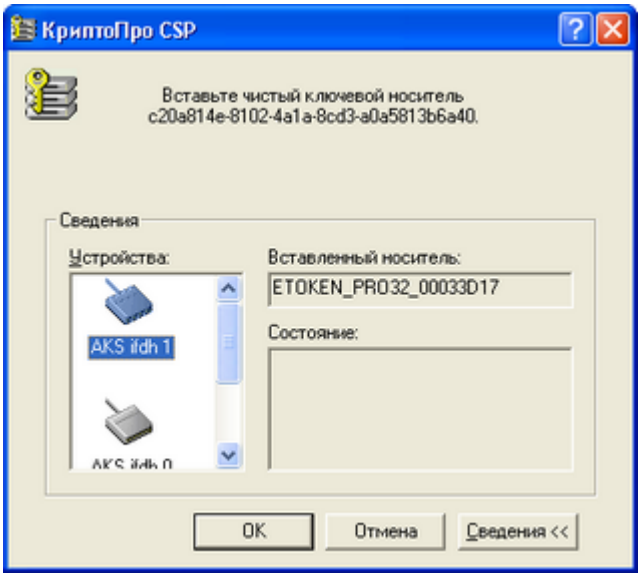


5. На следующей странице вам будет предложено выбрать параметры сертификата и ключевой пары.
   - В поле **Шаблон сертификата** выберите заранее созданный шаблон.
   - В поле CSP выберите из списка соответствующий алгоритм (один из выделенных на рисунке внизу).



6. Нажмите **Выдать**.
7. Убедитесь в том, что к компьютеру подключён только один eToken.

8. В окне **КриптоПро CSP** выберите считыватель, к которому подключён eToken, и нажмите **OK**.

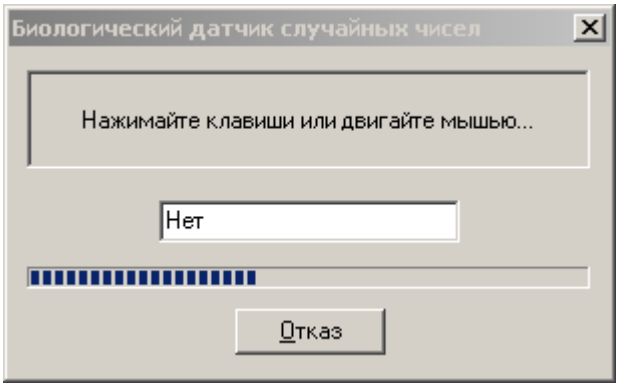


Примечание

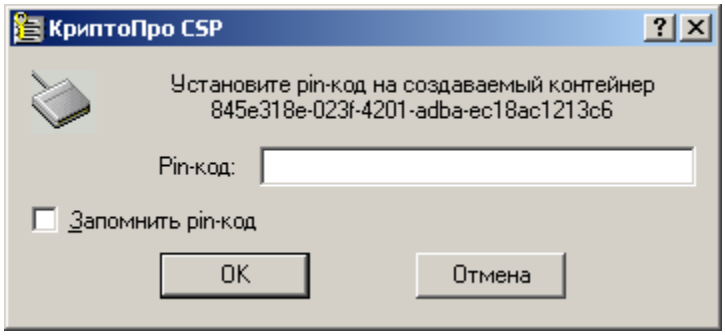
В поле Вставленный носитель отображается следующая информация: ETOKEN_<модель>_<идентификатор>, где <модель> =

- JAVA — для eToken GT, eToken PRO (Java) , eToken NG-FLASH (Java) и eToken NG-OTP (Java) ;
- PRO16 — для eToken PRO с операционной системой Siemens CardOS/M4.0;
- PRO32 — для eToken PRO с операционной системой Siemens CardOS/M4.01;
- PRO — для eToken NG-FLASH, eToken NG-OTP и eToken PRO с операционной системой Siemens CardOS V4.20 или 4.2b;

9. В следующем окне вам будет предложено инициализировать датчик случайных чиселю. Для этого двигайте мышью или нажимайте случайные клавиши на клавиатуре до тех пор, пока пунктирная шкала в окне не будет заполнена до конца.

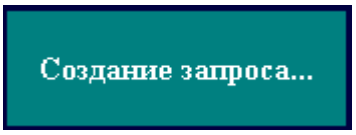


10. После инициализации датчика случайных чисел на экране автоматически появится окно для ввода ПИН-кода. Этот ПИН-код будет использоваться для доступа к создаваемому контейнеру.

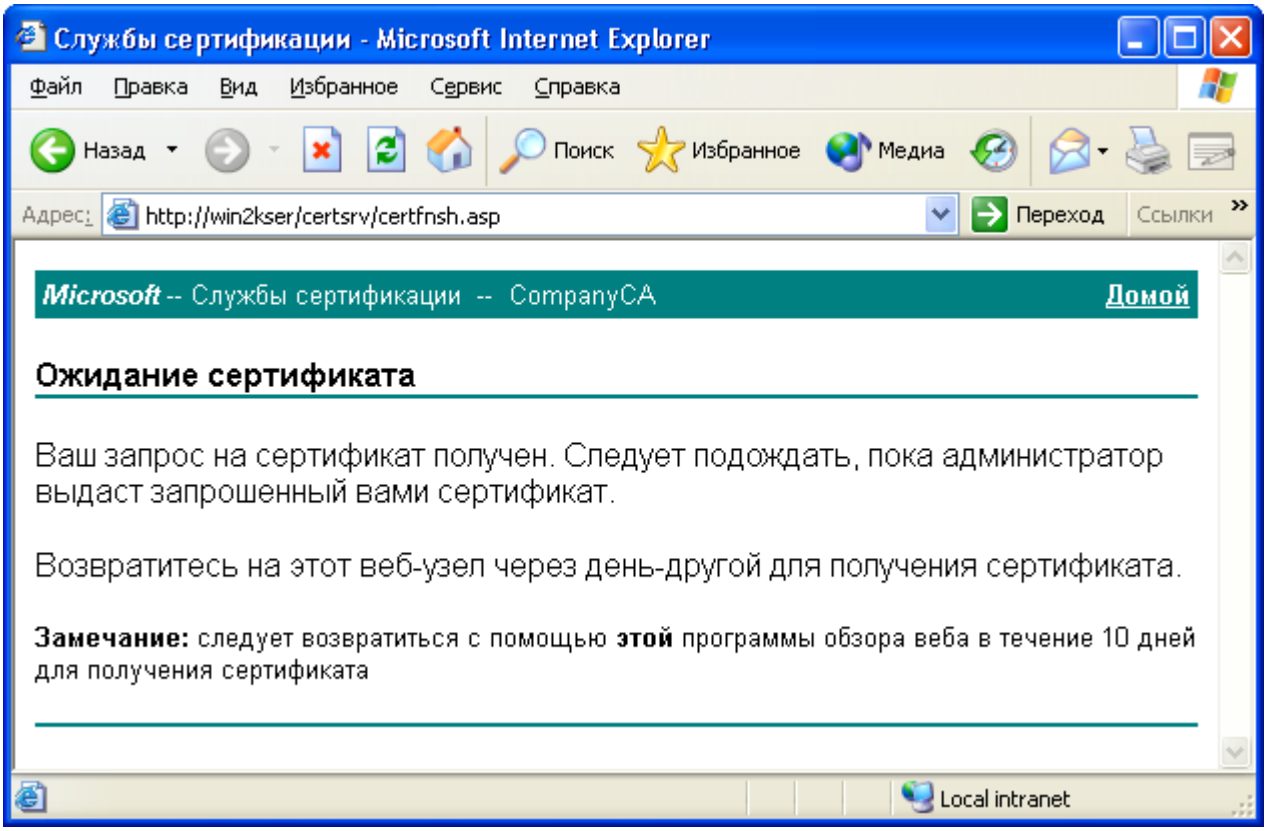


11. Нажмите **OK**. В памяти eToken будет создан ключевой контейнер КриптоПро CSP 3.6.

    В процессе подготовки запроса на получение сертификата в окне Internet Explorer будет отображаться следующее сообщение.

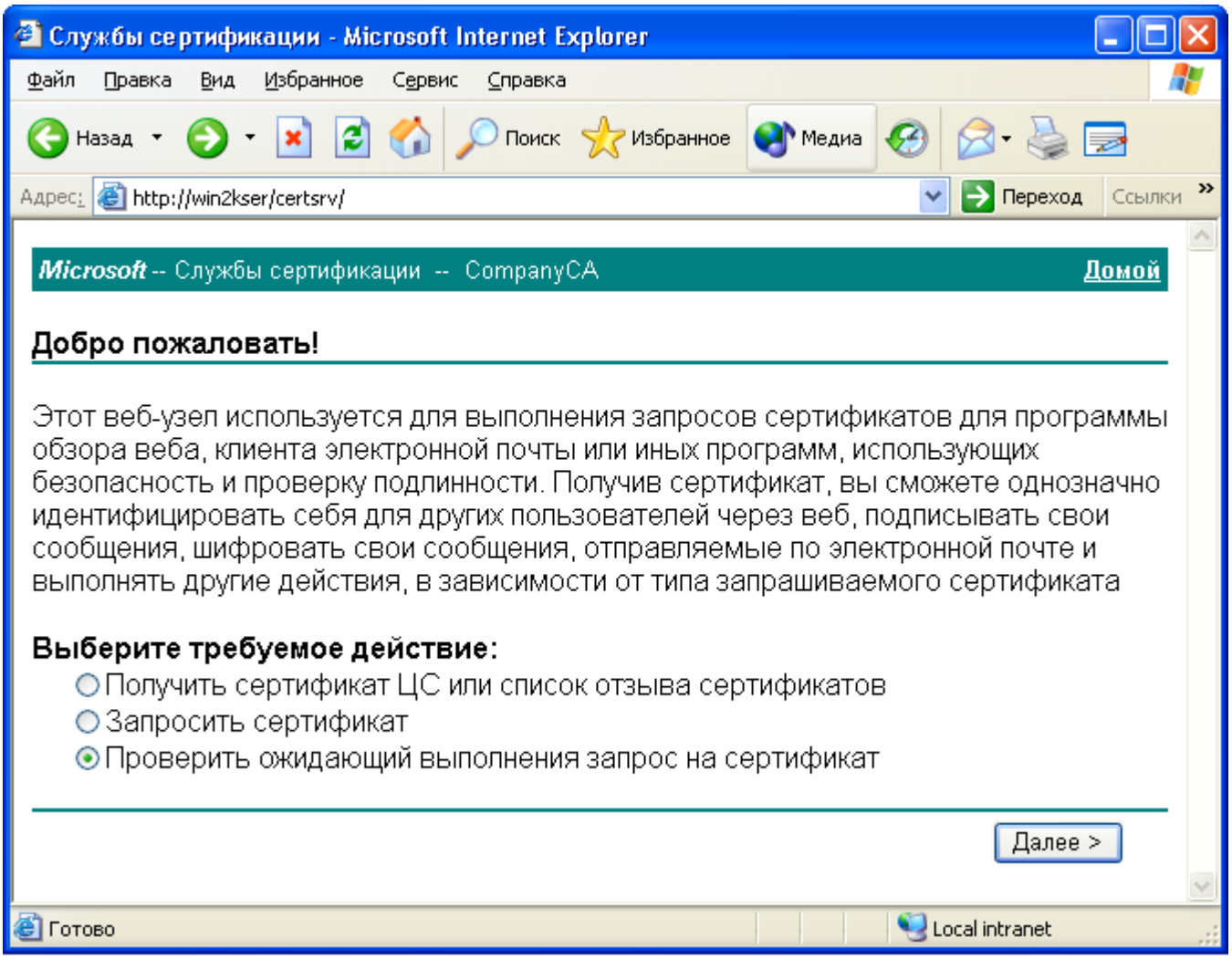


12. Если настройки центра сертификации требуют одобрения запрошенного сертификата диспетчером сертификатов, на экране появится страница **Ожидание сертификата/Certificate Pending**.

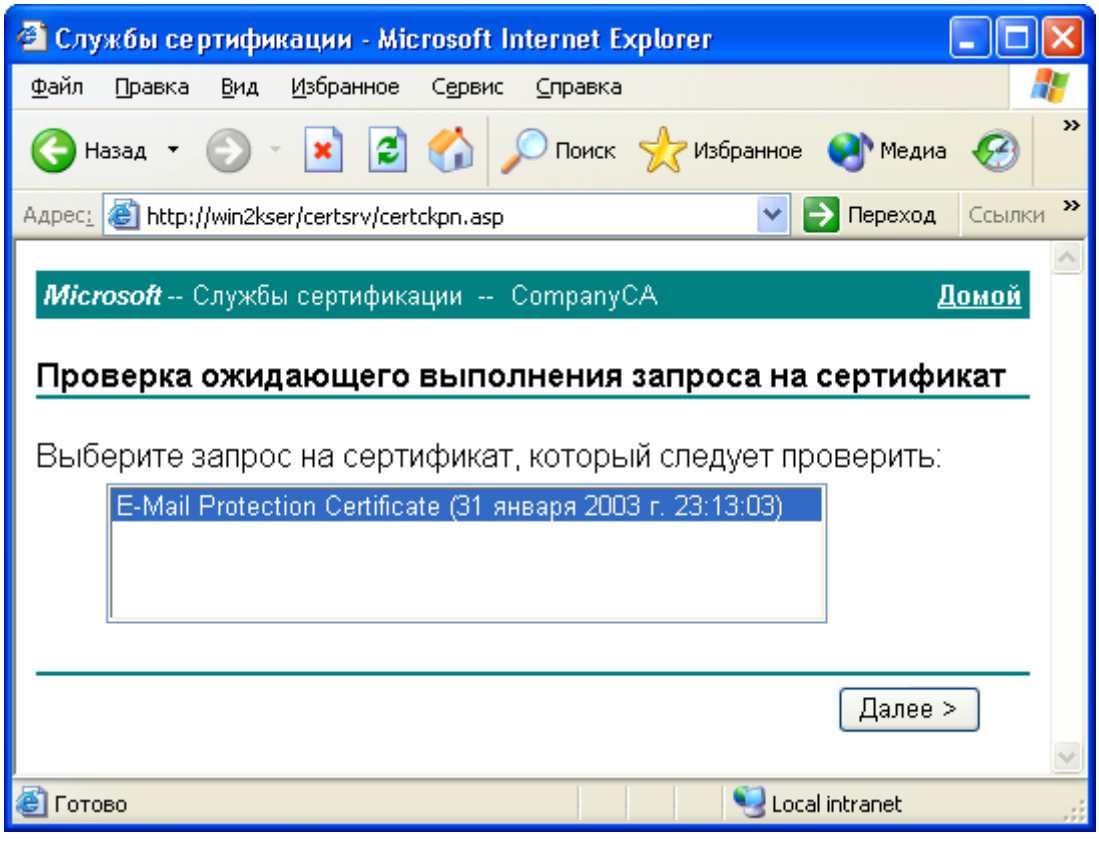


В этом случае:

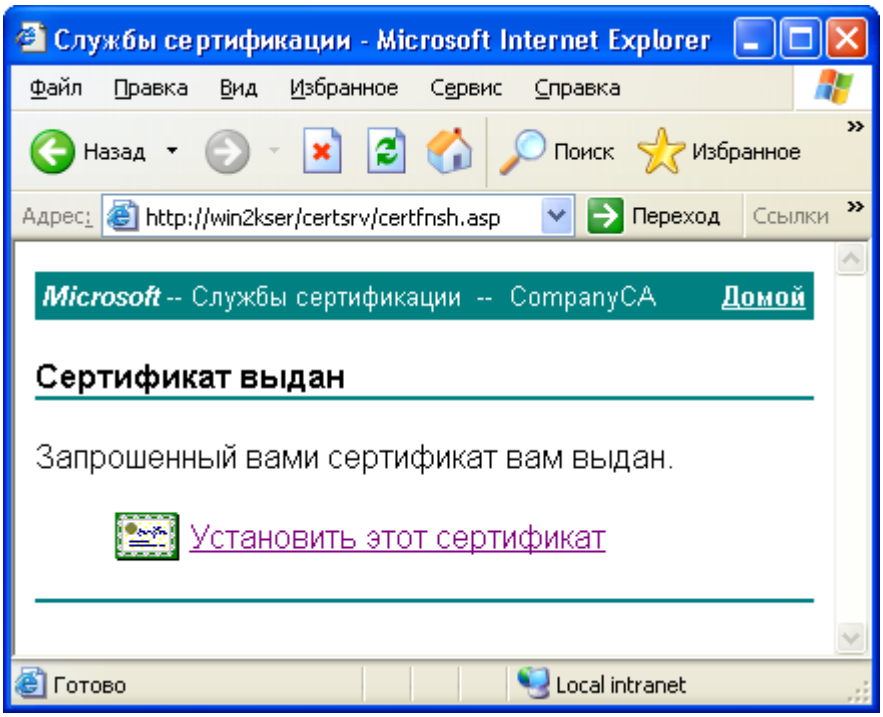
- дождитесь, пока диспетчер сертификатов выдаст запрошенный сертификат;
- на домашней странице веб-узла службы сертификации выберите **Проверить ожидающий выполнения запрос на сертификат/Check on a pending certificate** и нажмите **Далее/Next**;



- выберите запрос на сертификат, который следует проверить, и нажмите **Далее**/**Next**.

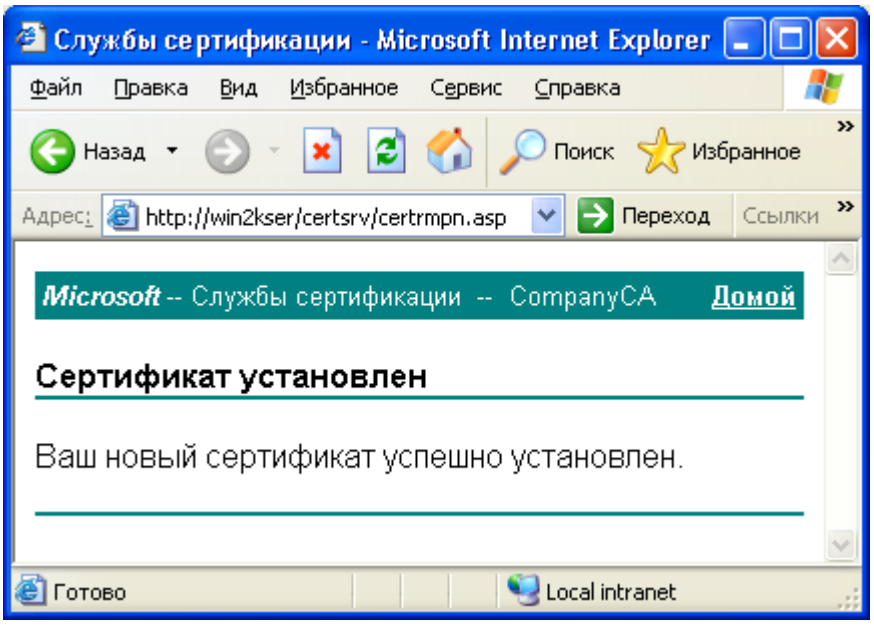


15. На странице **Сертификат выдан/Certificate Issued** нажмите **Установить этот сертификат/Install this certificate** для того чтобы установить сертификат в память eToken.



16. При необходимости в окне **КриптоПро CSP/CryptoPro CSP** для ввода ПИН-кода введите ПИН-код и нажмите **OK**.

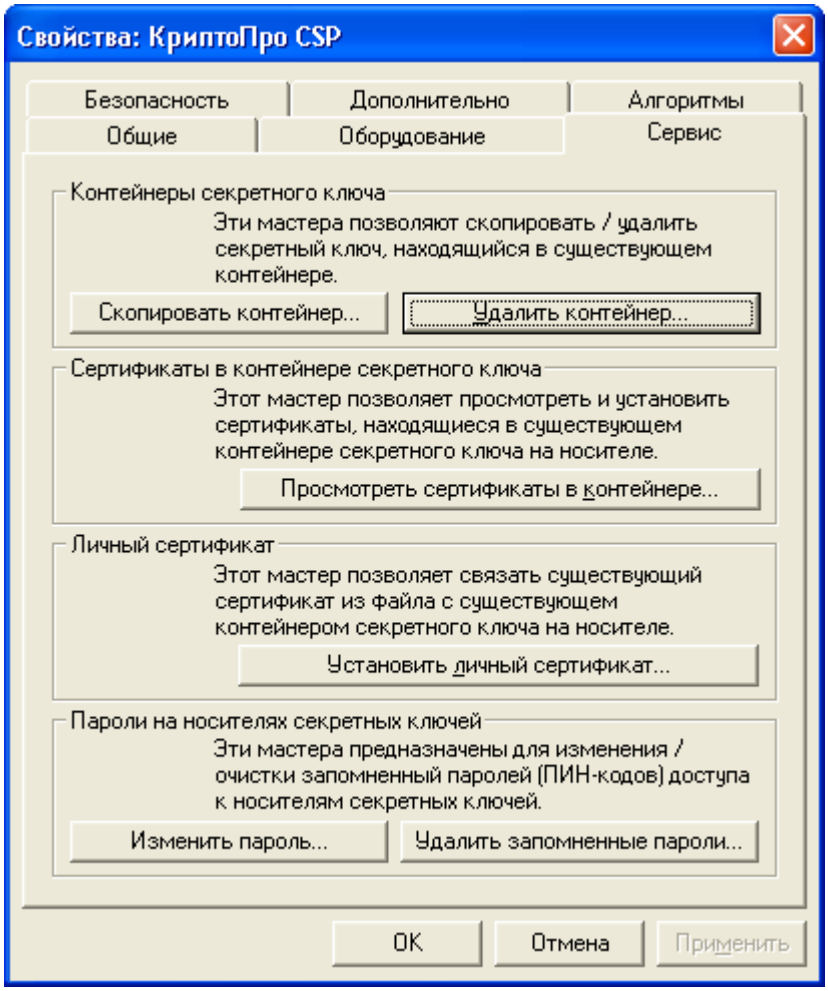
17. Убедитесь в том, что сертификат установлен: открылась страница **Сертификат установлен**.



Удаление ключевого контейнера из памяти eToken

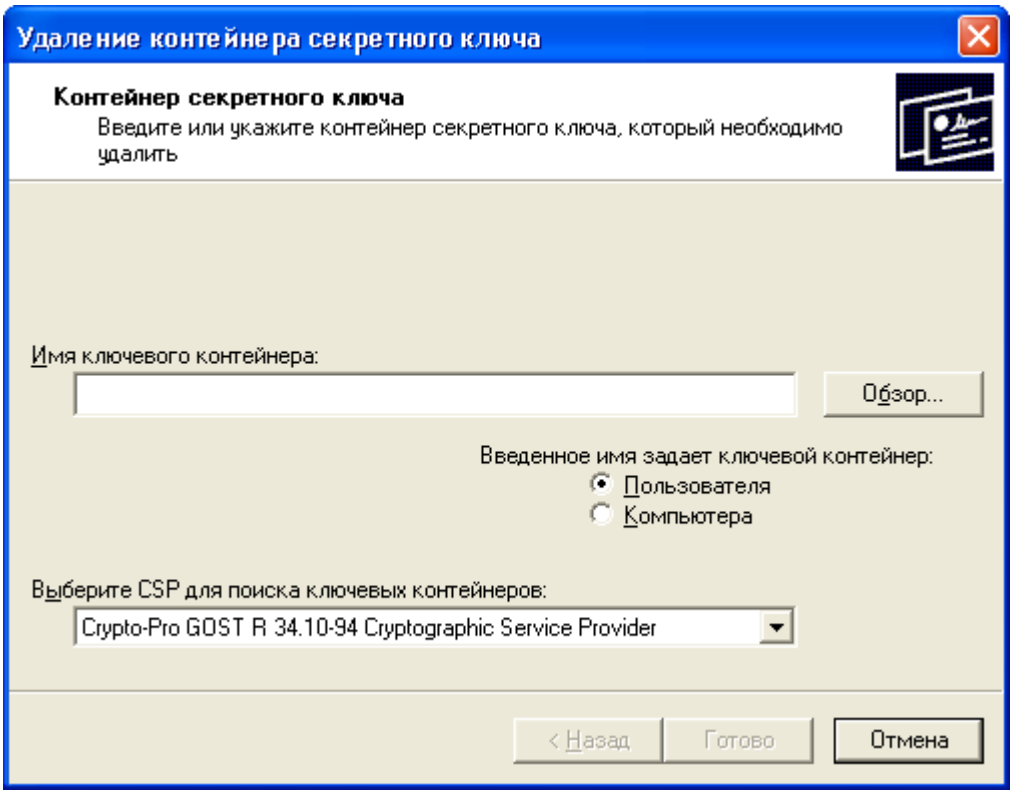
Для того чтобы удалить ключевой контейнер КриптоПро CSP из памяти eToken, выполните следующее.

1. Откройте **Панель управления**.
2. Если вы используете в Windows XP вид панели управления по категориям (category view), выберите **Прочие параметры панели управления**.
3. Выберите **КриптоПро CSP**.
4. В окне **Свойства: КриптоПро CSP** выберите вкладку **Сервис**.

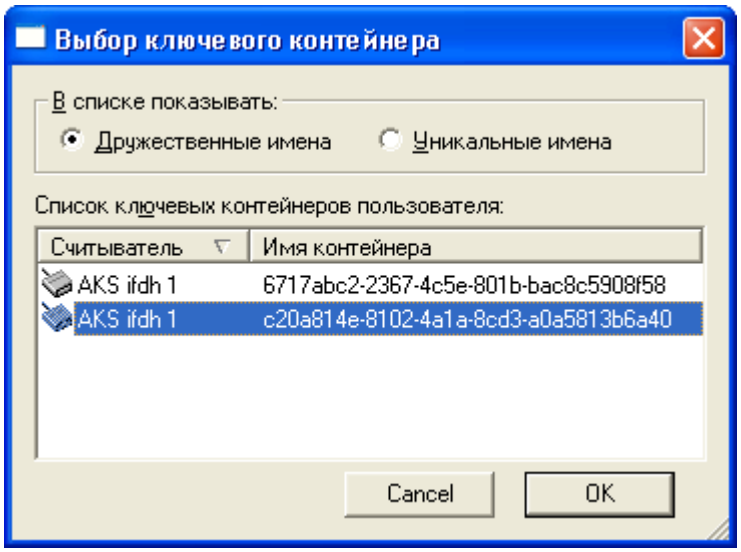


5. Нажмите **Удалить контейнер**.

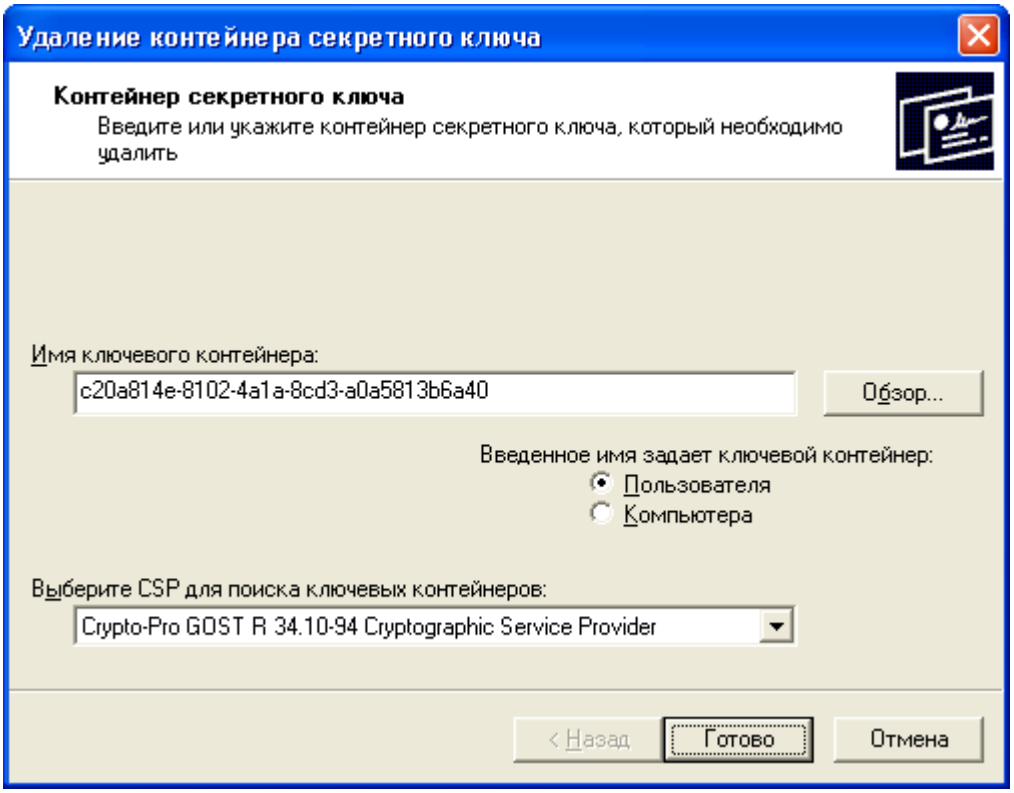
6. В окне **Удаление контейнера секретного ключа** нажмите **Обзор**.



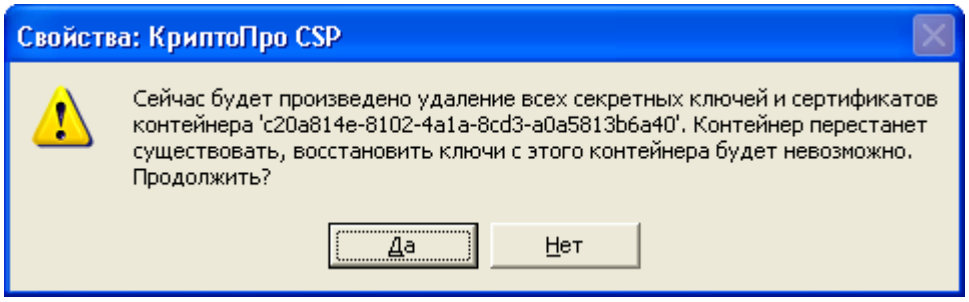
7. В окне **Выбор ключевого контейнера** выберите ключевой контейнер и нажмите **OK**.



8. В окне **Удаление контейнера секретного ключа** убедитесь в том, что имя выбранного контейнера появилось в поле **Имя ключевого контейнера**, и нажмите **Готово**.



9. В окне подтверждения нажмите **Да**.



10. При необходимости введите ПИН-код и нажмите **OK**.

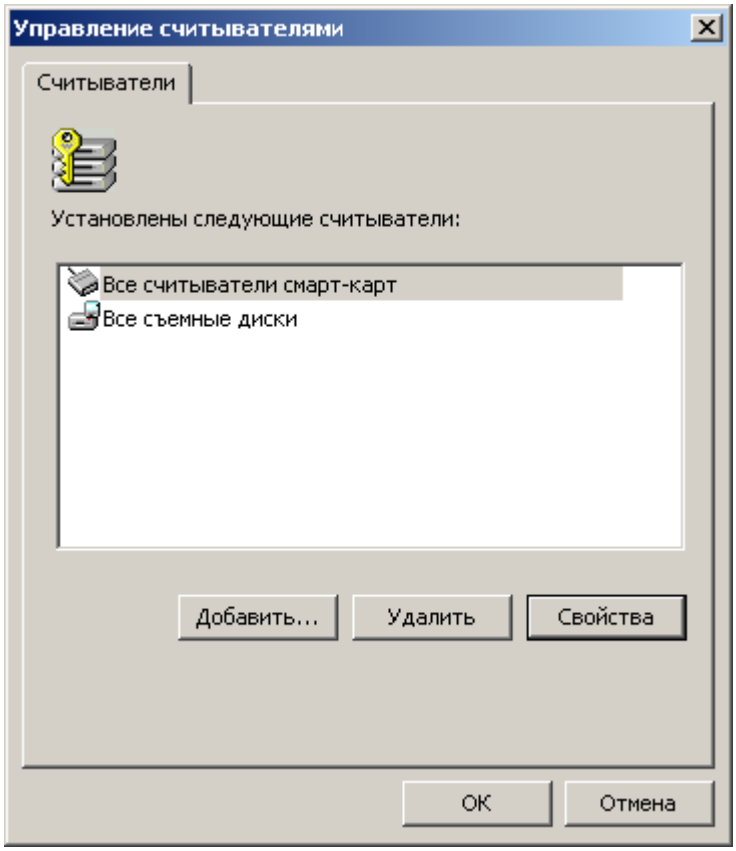
Удаление считывателей и носителей

Поскольку eToken для КриптоПро CSP 3.6 устанавливается только как обновление, то после его установки и настройки вы можете удалить только добавленные считыватели или носители.

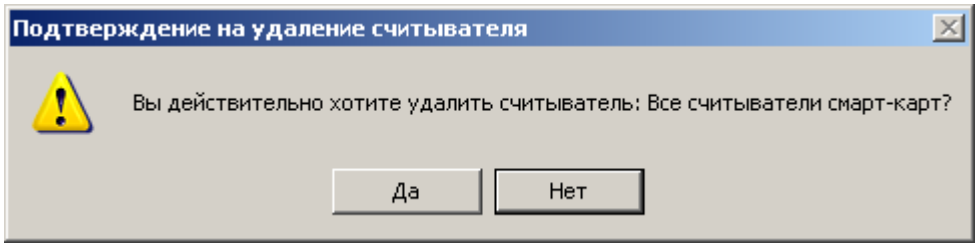
Удаление считывателей

Чтобы удалить считыватель, выполните следующие действия:

1. Откройте меню **Пуск > Панель управления > КриптоПро CSP**.
2. Во вкладке **Оборудование** нажмите кнопку **Настроить считыватели**. На экране откроется следующее окно.



3. Выберите требуемый считыватель и нажмите кнопку **Удалить**. На экране появится окно с запросом на подтверждение.

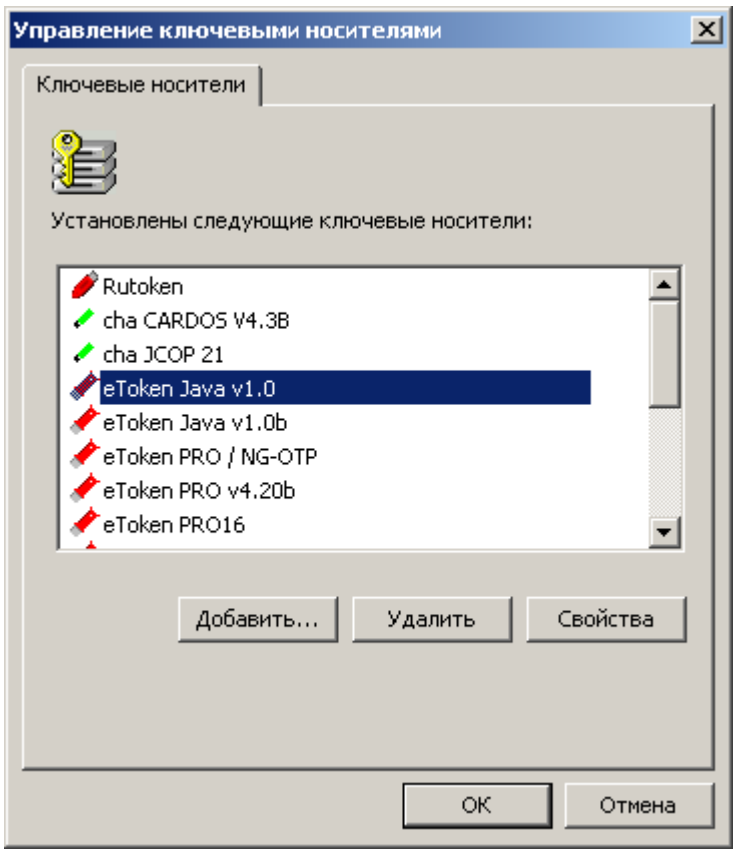


4. Нажмите **Да**, после чего выбранный считыватель будет удален из списка.

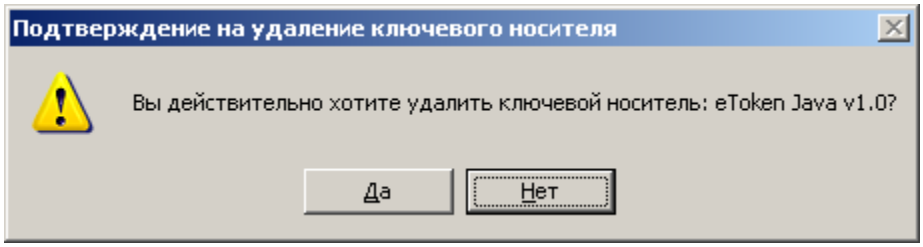
Удаление носителей

Чтобы удалить носитель, выполните следующие действия:

1. Откройте меню **Пуск > Панель управления > КриптоПро CSP**.
2. Во вкладке **Оборудование** нажмите кнопку **Настроить носители**. На экране откроется следующее окно.



3. Выберите требуемый носитель и нажмите кнопку **Удалить**. На экране появится окно с запросом на подтверждение.

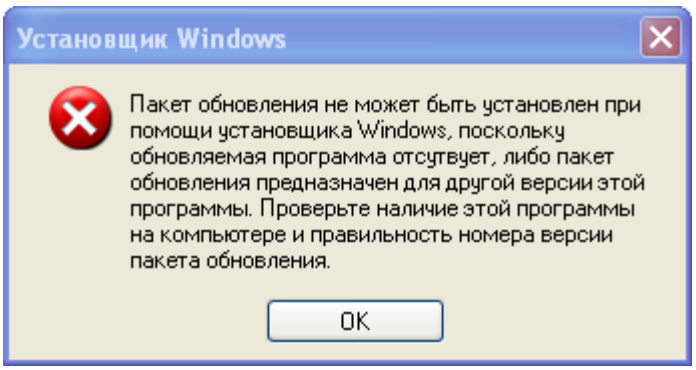


4. Нажмите **Да**, после чего выбранный носитель будет удален из списка.

Известные проблемы и их решение

Проблема:

При попытке установить «eToken для КриптоПро CSP 3.6» на экране появилось окно со следующим:



Возможная причина:

КриптоПро CSP 3.6 не установлен.

Решение:

Установите КриптоПро CSP 3.6. Руководство по установке можно найти на официальном сайте КриптоПро.

Проблема:

При добавлении в качестве носителя eToken на платформе Java, на экране появилось окно с сообщением:

Возможная причина:

Установлена устаревшая версия драйверов.

Решение:

Установите eToken PKI Client 5.1 SP1.

Проблема:

В окне **Управление считывателями** / **Readers' Control** во вкладке **Считыватели/Readers** кнопки **Добавить/Add** и **Удалить/Remove** неактивны.

Возможная причина:

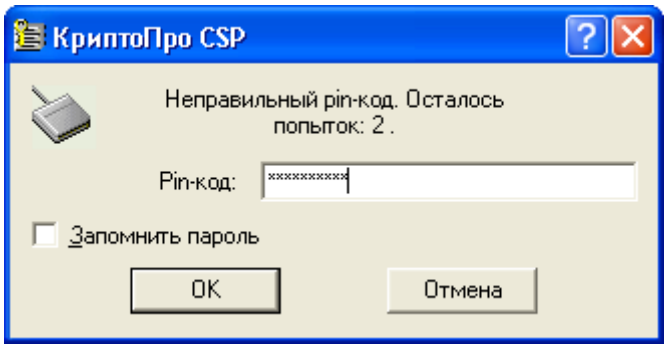
Вы не имеете полномочий локального администратора.

Решение:

Настраивать считыватели могут только пользователи, наделённые полномочиями локального администратора. Без этих полномочий настройка невозможна. Нажмите **Отмена/Cancel**.

Проблема:

После ввода ПИН-кода на экране появилось окно **КриптоПро CSP/CryptoPro CSP** для ввода ПИН-кода с сообщением о введении неправильного ПИН-кода и указанием числа оставшихся попыток ввода ПИН-кода.



Возможные причины:

1. Вы неверно ввели ПИН-код.
2. К компьютеру подключён другой eToken.
3. eToken был отключен.

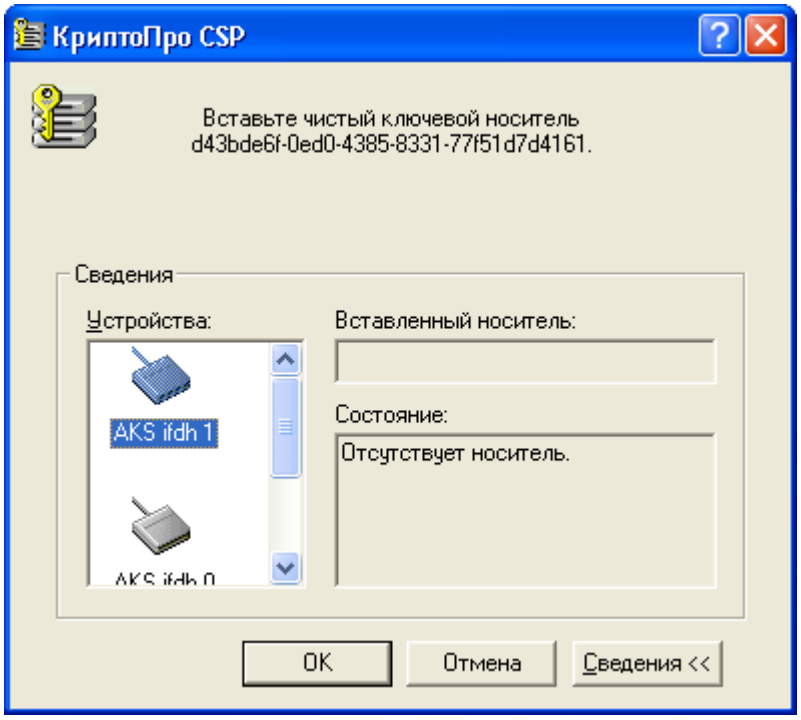
Решение:

1. Проверьте правильность введенного ПИН-кода.
2. Убедитесь в том, что вы вводите ПИН-код именно того eToken, который подключен к компьютеру. Помните, что количество последовательных попыток ввода неверного ПИН-кода ограничено, и превышение этого ограничения ведет к блокированию устройства eToken.
3. Подключите eToken, если он был отключен.

Проблема:

При установке сертификата в появившемся окне КриптоПро CSP поле **Вставленный носитель** остается пустым, а в поле **Состояние/Status** отображается сообщение:

```
Отсутствует носитель/No carrier.
```



Возможные причины:

1. Вы неверно выбрали считыватель
2. eToken не подключён к компьютеру.

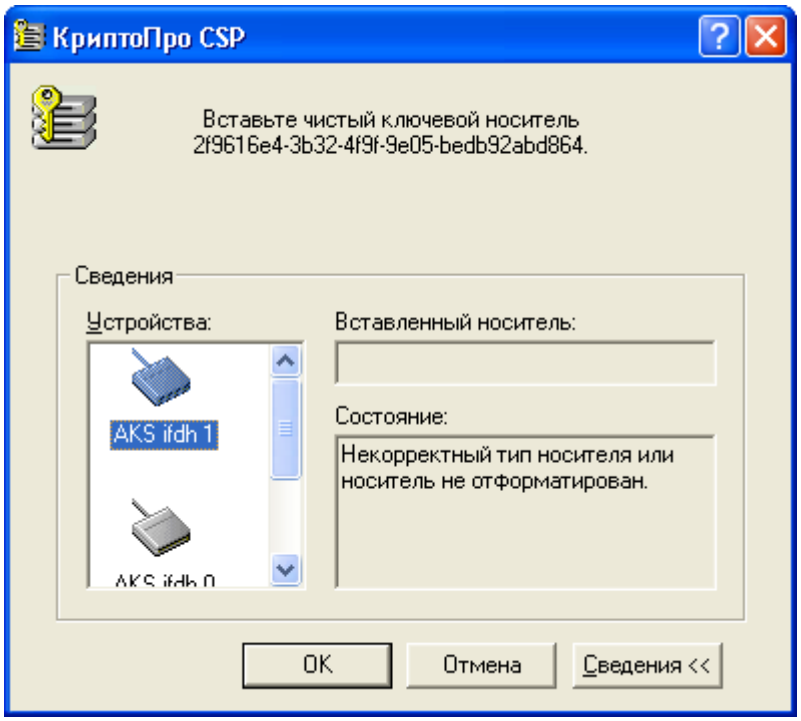
Решение:

1. Убедитесь в том, что вы верно выбрали считыватель.
2. Убедитесь в том, что eToken подключен к компьютеру. У USB-ключа eToken должен гореть световой индикатор. Такой же индикатор должен гореть на считывателе, если вы пользуетесь смарт-картой eToken.

Проблема:

После выбора считывателя в списке **Устройства/Readers** в окне **КриптоПро CSP** в поле **Состояние** отображается сообщение:

`Некорректный тип носителя или носитель не отформатирован / Invalid carrier media or carrier media not supported.`



Возможные причины:

1. eToken для КриптоПро CSP 3.6 не установлен.
2. После установки eToken для КриптоПро CSP 3.6 компьютер не был перезагружен.

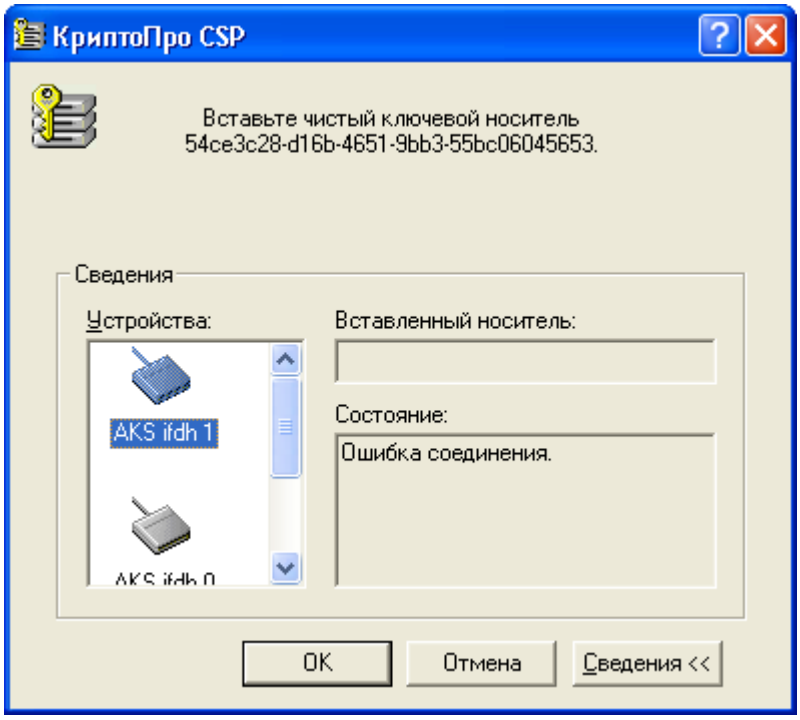
Решение:

1. Нажмите **OK**.
2. Убедитесь в том, что eToken для КриптоПро CSP 3.6 установлен. Если это не так, установите eToken для КриптоПро CSP 3.6.
3. Перезагрузите компьютер.

Проблема:

При попытке записать сертификат в память eToken в окне **КриптоПро CSP** в поле **Состояние/Status** отображается сообщение:

```
Ошибка соединения / Connection error.
```



Возможная причина:

Не установлен набор драйверов eToken RTE или eToken PKI Client.

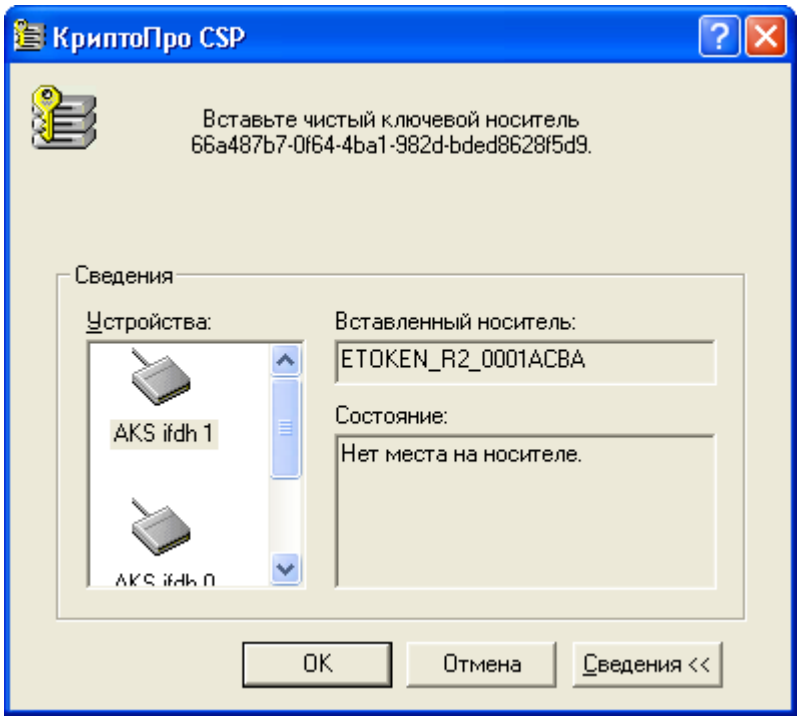
Решение:

Установите eToken RTE или eToken PKI Client.

Проблема:

В процессе установки сертификата в eToken в окне **КриптоПро CSP** в поле **Состояние** отображается сообщение:

```
Нет места на носителе/Carrier full.
```



Возможные причины:

1. Недостаточно памяти eToken.
2. Достигнуто ограничение по количеству ключевых контейнеров, которые могут храниться в памяти eToken.

Решение:

1. Удалите из памяти eToken ненужные объекты.
2. При использовании eToken в качестве носителя ключевых контейнеров КриптоПро CSP действует ограничение на максимально возможное количество конетейнеров: по умолчанию в памяти eToken можно сохранить не более 10 контейнеров. В некоторых случаях требуется использовать более чем 10 ключевых контейнеров.В описании носителей eToken в КриптоПро CSP "жестко" прописаны папки хранения ключевых контейнеров, по умолчанию их 10.

   Можно изменить описание носителя eToken, добавив в параметре Folders папки CC10 - CC19.

   Ниже приведён пример ветки реестра для носителя eToken PRO 32k:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\KeyCarriers\eToken_PRO32\Default]

   "Folders"="CC00\\CC01\\CC02\\CC03\\CC04\\CC05\\CC06\\CC07\\CC08\\CC09"

   Количество папок можно увеличить, ветка реестра для этого носителя будет выглядеть так:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\KeyCarriers\eToken_PRO32\Default]

   "Folders"="CC00\\CC01\\CC02\\CC03\\CC04\\CC05\\CC06\\CC07\\CC08\\CC09\
   \CC10\\CC11\\CC12\\CC13\\CC14\\CC15\\CC16\\CC17\\CC18\\CC19"

   Важно помнить, что память eToken ограничена, а размер ключевых контейнеров КриптоПро CSP, как правило, в несколько раз больше, чем размер ключевого контейнера RSA-сертификата с соответствующим ему закрытым ключом.

   eToken с объемом памяти 32k в среднем может быть помещено порядка 8-10 ключевых контейнеров КриптоПро CSP, на eToken с объемом памяти 64к – порядка 17-19 ключевых контейнеров КриптоПро CSP.

Проблема:

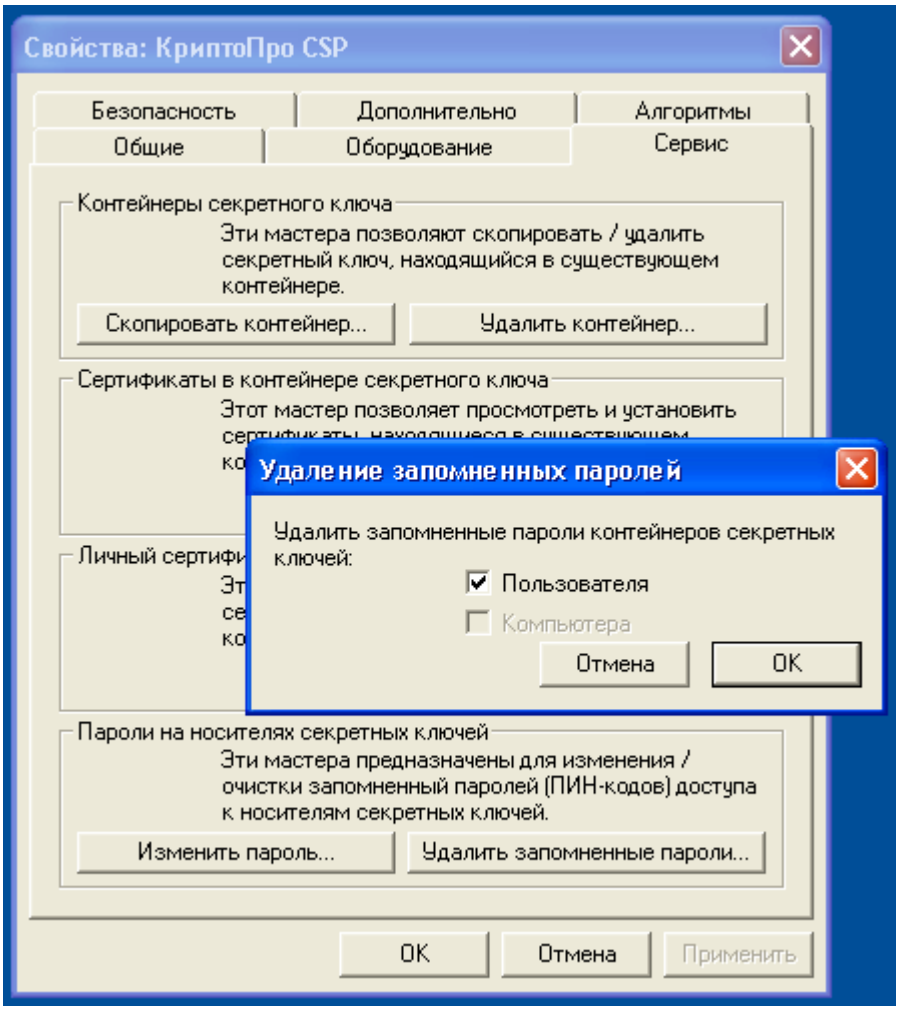
На экране появилось сообщение о том, что в контейнере отсутствуют секретные ключи.

Возможная причина:

Сохраненный ПИН-код eToken был изменён.

Решение:

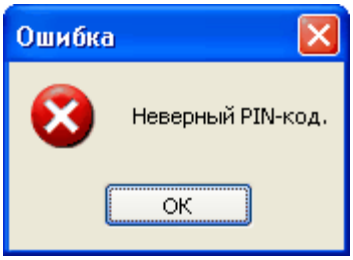
Удалите сохраненные пароли ключевых контейнеров КриптоПро CSP 3.6.



Проблема:

На экране появилось окно **Ошибка/Error** с сообщением:

```
Неверный ПИН-код
```



Возможная причина:

Вы неверно ввели ПИН-код выбранного eToken.

Решение:

Нажмите **OK** и повторите попытку.

Тел: (495) 223-0001
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru