Утилита экспорта ключевой пары CSP в контейнер PKCS#12
Руководство пользователя

21 декабря 2011 г.

Оглавление

1 Введение

Утилита экспорта ключевой пары CSP в контейнер **PKCS#12** предназначена для создания резервной копии личного сертификата пользователя вместе с закрытым ключом, хранящихся в контейнере криптопровайдера (CSP) с поддержкой российской криптографии (ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001). Резервная копия создаётся в защищенном контейнере **PKCS#12**.

Экспорт возможен только для контейнеров с разрешённой операцией экспорта (флаг CRYPT_EXPORT).

PKCS#12 — формат для переноса сертификата и связанного с ним закрытого ключа с машины на машину или для резервного копирования. В этом формате могут также содержаться сертификаты удостоверяющего центра.

Файлы формата **PKCS#12** всегда кодируются в формате DER. Эти файлы требуют особенно пристального внимания, поскольку содержат закрытый ключ; при неосторожном обращении с таким файлом закрытый ключ легко скомпрометировать. Как правило, эти файлы защищены на пароле. Расширение файлов формата **PKCS#12** либо «.p12», либо «.pfx».

Содержимое контейнера **PKCS#12**, полученного путём использования утилиты, можно импортировать и использовать в любых приложениях. Их можно импортировать в **LISSI-CSP**, в **Firefox**, **Thunderbird** или **SeaMonkey**, использовать в приложениях, написанных на **NSS** и **OpenSSL 1.x.x** с подключенным **engine ccgost** от ООО «КриптоКом» или одним из **engine** семейства «**lc_**» от ООО «ЛИССИ-Крипто» и т.д.

Для использования сохраненного в контейнере **PKCS#12** личного сертификата и закрытого ключа при переходе, например, на использование **LISSI-CSP** достаточно, после установки **LISSI-CSP**, щелкнуть два раза по контейнеру и выполнить процедуру импорта. В результате ваш личный сертификат и закрытый ключ будут установлены в систему.

Получив с помощью утилиты контейнер **PKCS#12** можно также сохранить личный сертификат и закрытый ключ на программном или аппаратном токене с неизвлекаемым ключом, например на **RuToken ЭЦП**. Для этого вы можете воспользоваться программным комплексом **RusXCA**.

Также при переносе личного сертификата и закрытого ключа на другой компьютер, потребуется перенести или скачать корневой сертификат центра сертификации, выдавшего сертификат.

2 Процесс экспорта

Для получения резервной копии достаточно проделать следующие действия:

- запустить утилиту
- выбрать личный сертификат и нажать кнопку «**OK**»

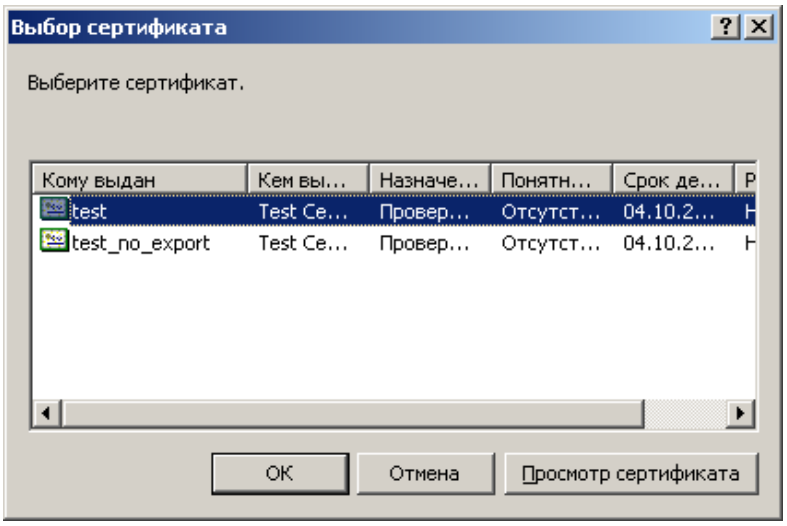

Рис. 2.1

***Примечание**: Если у выбранного контейнера CSP отсутствует флаг экспорта появится следующее сообщение об ошибке. В этом случае экспорт сертификата невозможен.*

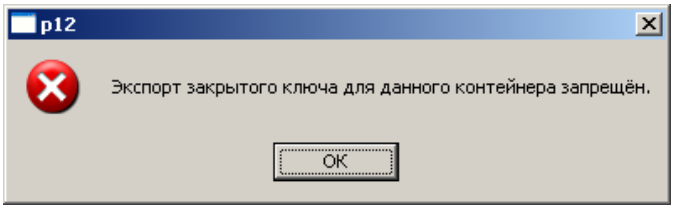

Рис. 2.2

- ввести пароль на контейнер CSP

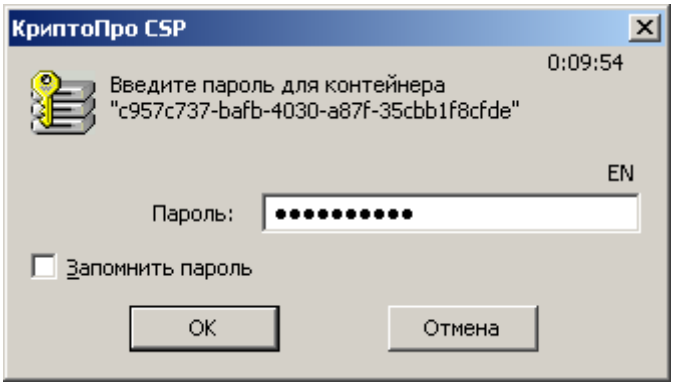

Рис. 2.3

- задать пароль на контейнер PKCS#12

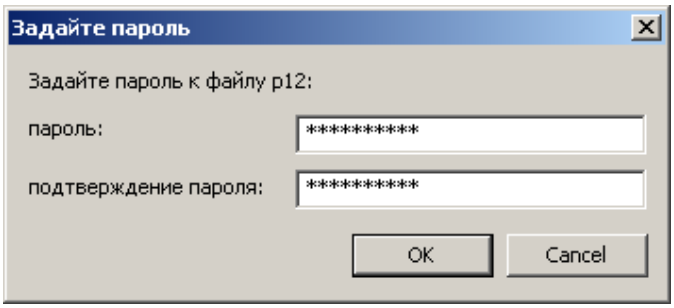

Рис. 2.4

- задать имя и путь файла для контейнера PKCS#12

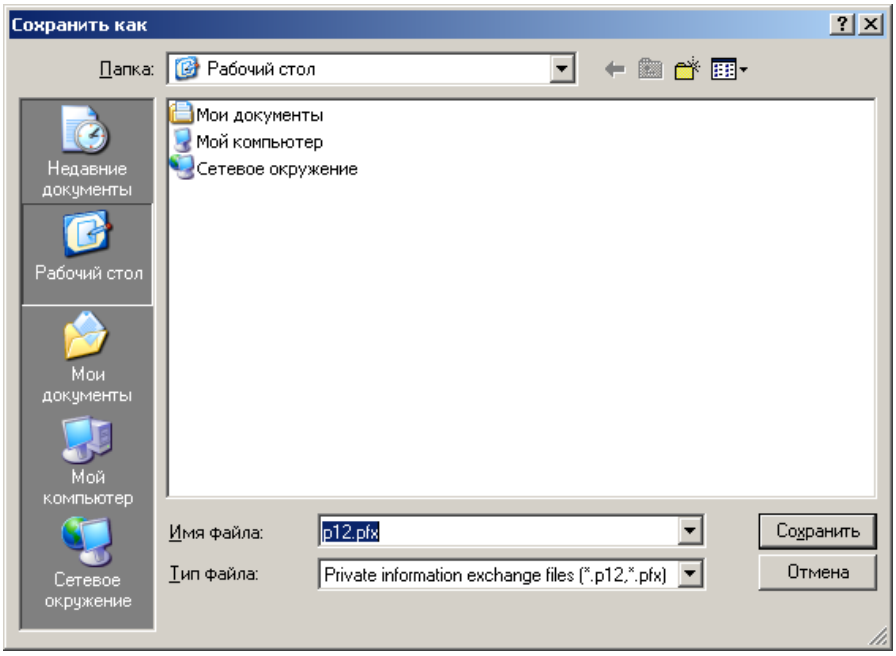

Рис. 2.5

- после нажатия кнопки «**Сохранить**» контейнер PKCS#12 будет сохранен в файле с заданным именем

3 Экспорт сертификата центра сертификации

При импорте контейнера PKCS#12 вам также понадобится установить сертификат центра сертификации, в том случае если он ещё не установлен. Его можно либо загрузить с сайта центра сертификации, либо перенести с компьютера на котором он уже установлен.

Для экспорта сертификата центра сертификации достаточно проделать следующие действия:

- запустить браузер **Internet Explorer** (для этого достаточно выполнить команду «Пуск | Все программы | Internet Explorer»)
- выполнить команду меню «Сервис | Свойства обозревателя»

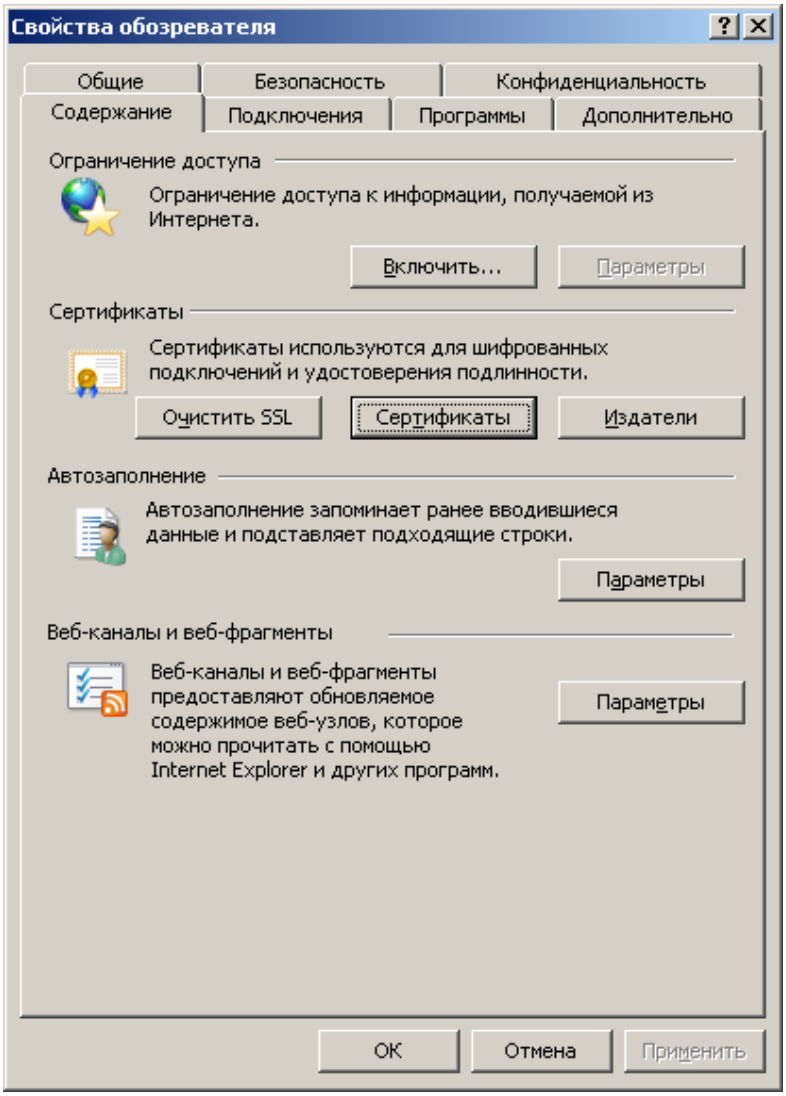

Рис. 3.1

- в появившемся диалоговом окне следует выбрать вкладку «Содержание» и нажать кнопку «Сертификаты». В следующем диалоге следует выбрать вкладку «**Личные**» и два раза щелкнуть левой кнопкой мыши по нужному сертификату

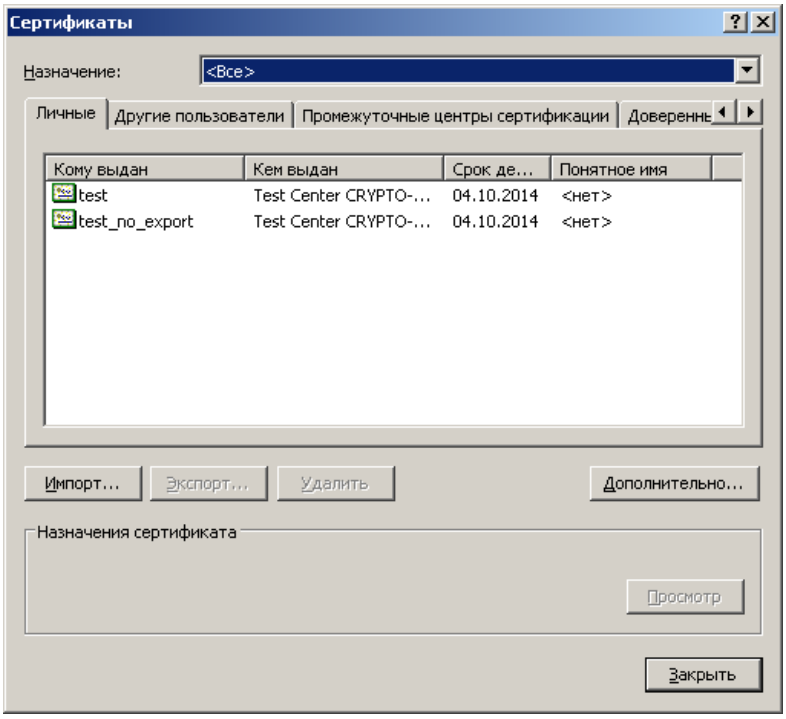

Рис. 3.2

- в появившемся окне следует выбрать вкладку «Путь сертификации» и дважды щелкнуть по сертификату центра сертификации

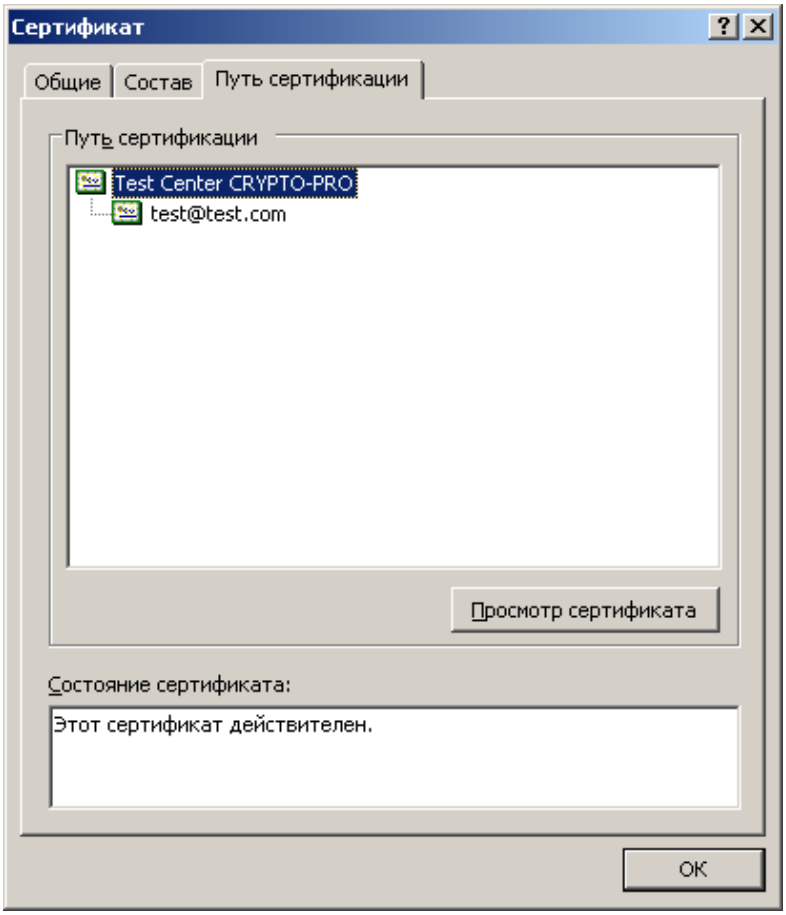

Рис. 3.3

- в следующем окне необходимо выбрать вкладку «Состав» и нажать кнопку «Копировать в файл...»

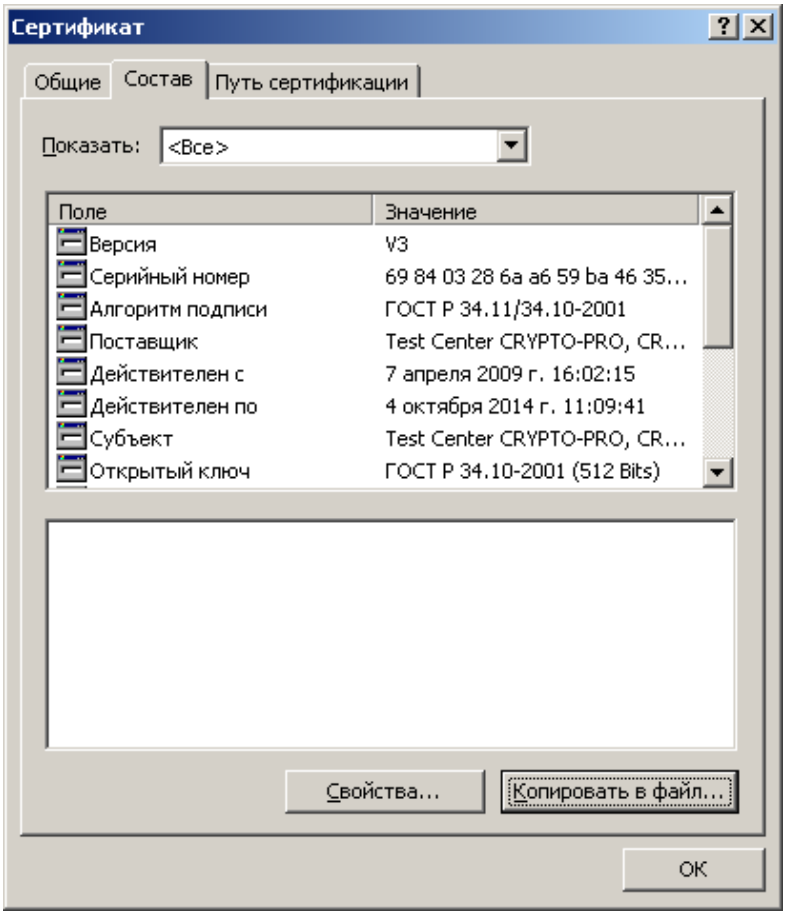

Рис. 3.4

- после этого необходимо следовать инструкциям мастера экспорта сертификата

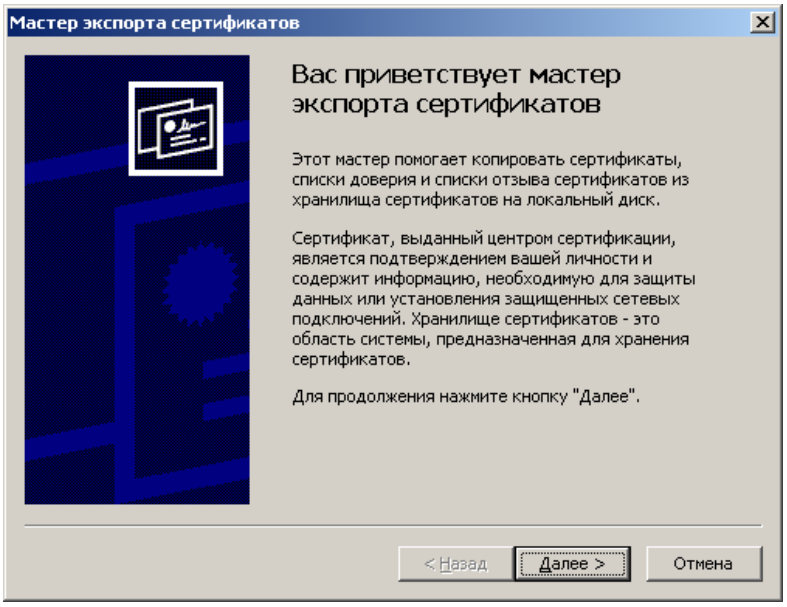

Рис. 3.5

- задать формат файла сертификата - **Файлы в DER-кодировке X.509 (.CER)**

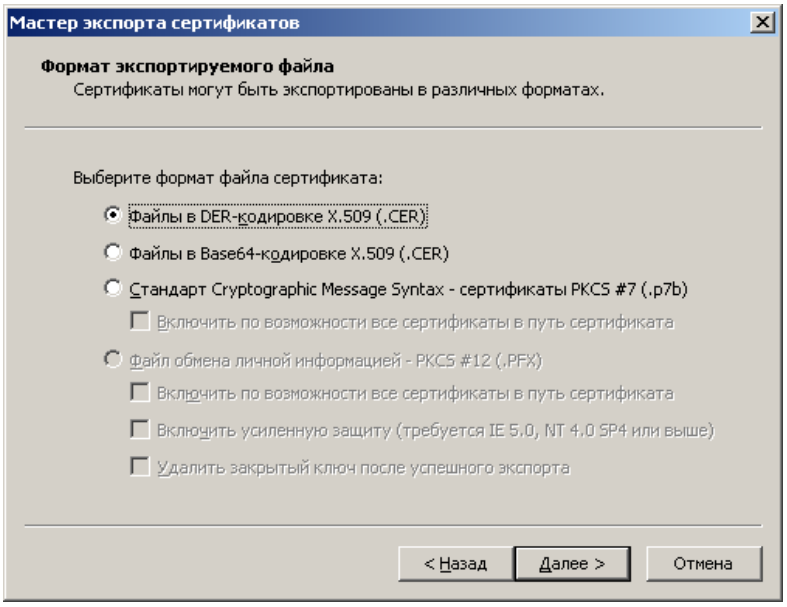

Рис. 3.6

- задать путь и имя файла с помощью кнопки «Обзор»

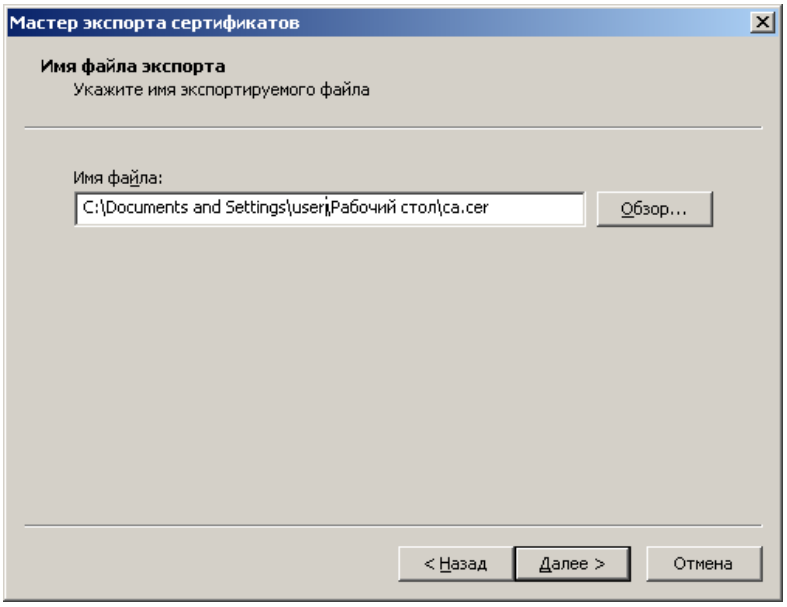

Рис. 3.7

- нажать кнопку «Готово»

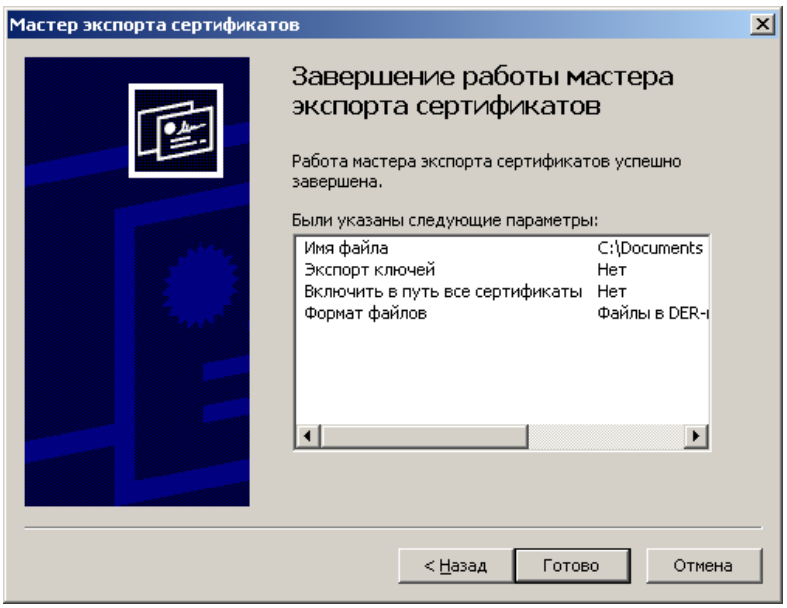

Рис. 3.8

- появится сообщение об успешном экспорте сертификата в выбранный файл

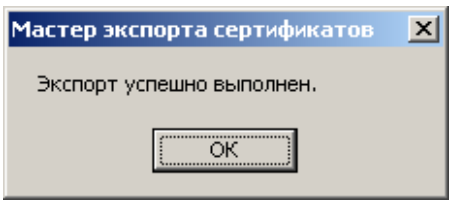
Мастер экспорта сертификатов
Экспорт успешно выполнен.
OK

Рис. 3.9