ESMART®

EFS-шифрование в Windows с сертификатом на ESMART Token

для Windows XP, Vista, 7 и 8
выпуски
Professional, Ultimate или Enterprise

Содержание

1. Шифрование Windows EFS

*Шифрование папок и файлов в Windows используется для их защиты от нежелательного доступа. Шифрованная файловая система (**Encrypted File System**) — это компонент Windows, позволяющий хранить сведения на жестком диске в зашифрованном виде.*

В базовых и домашних версиях Windows XP, Vista, Windows 7 и Windows 8 EFS шифрование поддерживается только частично через командную строку.

1.1 Преимущества EFS

- *Защита конфиденциальной информации на ПК: если ПК используется несколькими пользователями, EFS ограничивает доступ других пользователей к конфиденциальным файлам;*
- *Безопасное хранение ключей: в Windows Vista и выше появилась возможность хранить ключи EFS-шифрования на смарт-картах и USB-ключах;*
- *Централизованное управление: в Windows Vista и выше можно управлять политикой защиты централизованно, используя консоли локальной и доменной групповой политики.*

1.2 Уязвимость EFS

- *Совместимость только с NTFS: если пользователь, обладающий закрытым ключом, переносит файл или папку с файлами на раздел или внешний носитель FAT, данные будут автоматически дешифрованы, но пользователь может даже не узнать об этом.*
- *Хранение ключей EFS в системе: хранение ключа расшифровки в системе может позволить злоумышленнику получить доступ к данным, зная пароль к учетной записи пользователя. Перенос ключа дешифрования на смарт-карту ESMART Token позволяет решить эту проблему.*
- *Режим гибернации или спящий режим: если пользователь авторизовался на ПК, не заблокировал учетную запись и перешел в спящий режим или режим гибернации, злоумышленник может войти под его учетной записью и скопировать файлы. Проблема решается настройкой принудительного выхода из системы и использованием смарт-карт или USB-ключей ESMART Token (без кэширования ключей).*
- *Использование агента восстановления данных (Data Recovery Agent, DRA). DRA используется для получения доступа к зашифрованным данным в случае утери пользователем ключей или других экстренных случаях. Желательно хранить сертификат DRA с закрытым ключом на защищенном внешнем носителе, например, смарт-карте или USB-ключе ESMART Token.*

2. Подготовка к работе

Подключите к ПК считыватель и установите драйвера.

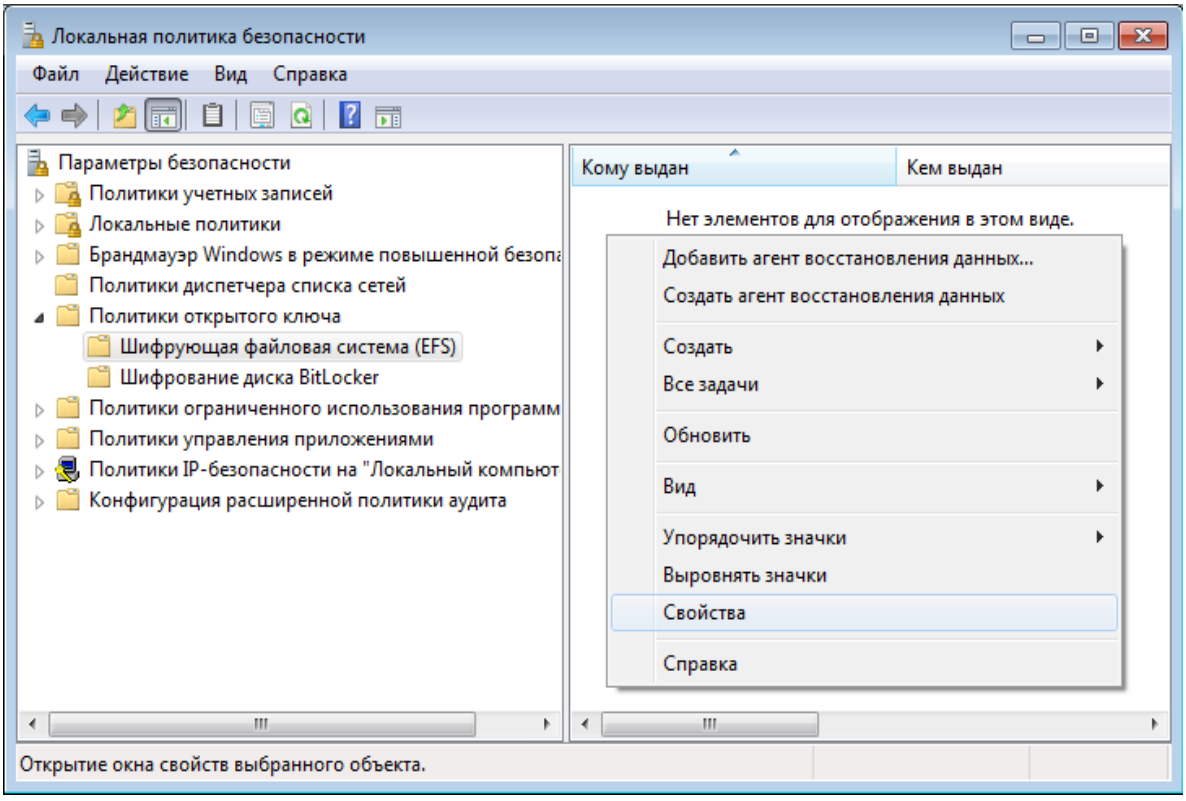
Для работы с картами и токенами ESMART Token в Windows требуется установка криптопровайдера. Процедура автоматической установки описана в руководстве администратора ESMART PKI Client, ручная установка отдельных компонентов описана в руководстве ESMART Token - CSP. Требуются права администратора.

3. Настройка EFS

Ключи и сертификаты шифрования EFS, начиная с Windows Vista, можно хранить на смарт-картах или USB-ключах, что позволяет защитить закрытый ключ от копирования или использования посторонними. Это особенно важно для портативных компьютеров и рабочих станций с общим доступом. Использование смарт-карт для хранения ключей шифрования позволяет улучшить управление ключами в крупных организациях.

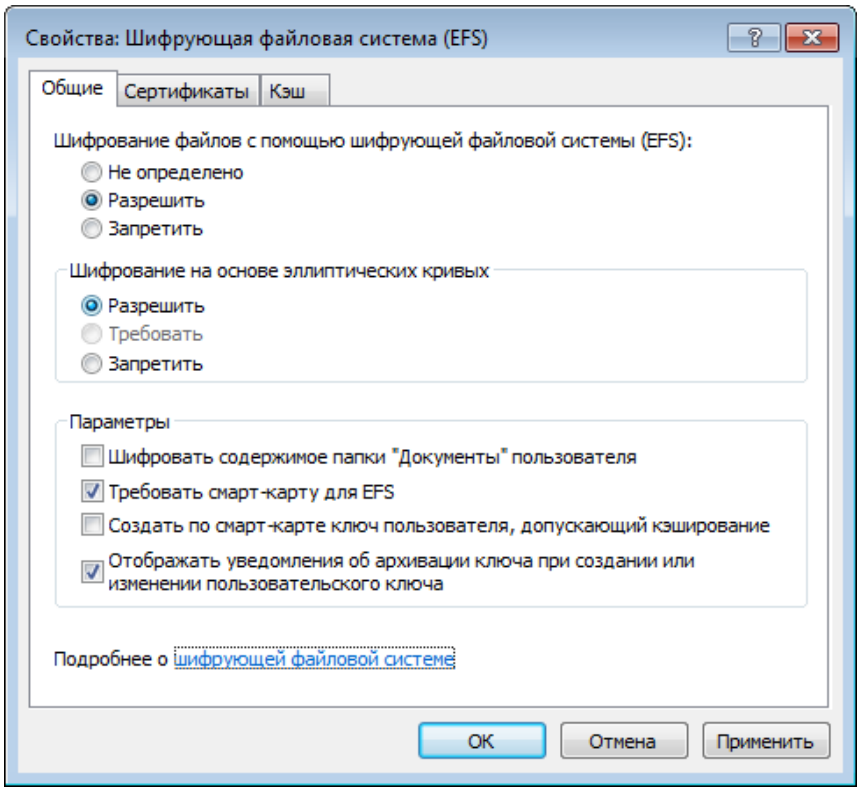
Преимуществом использования смарт-карты для хранения сертификата и ключей EFS является то, что смарт-карта защищена от подбора ПИН-кода путем перебора.

Настроить параметры файловой системы EFS можно с помощью консоли управления локальными групповыми политиками (gpedit.msc) или локального редактора политик безопасности (secpol.msc). Доменная групповая политики настраивается таким же образом, как и локальная. Чтобы просмотреть или изменить эти параметры, разверните узел ***Политики открытого ключа****, щелкните правой кнопкой мыши элемент* ***Шифрованная файловая система*** *и выберите пункт* ***Свойства****.*

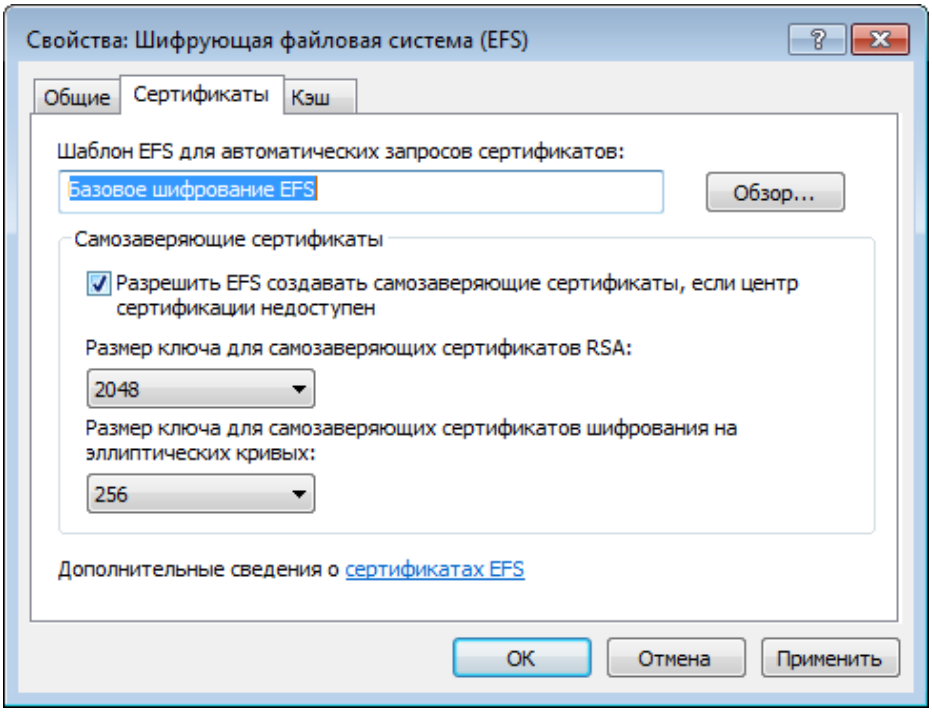


На вкладке ***Общие*** *можно разрешить или запретить EFS-шифрование на локальном уровне.*

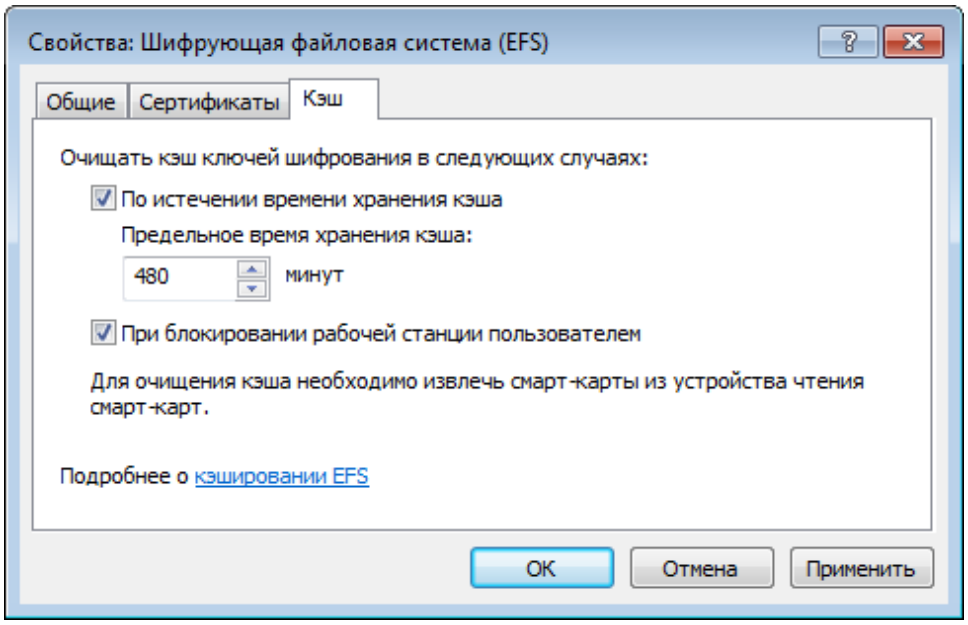
Включение или отключение шифрования на основе эллиптических кривых (ECC) требуется для соответствия стандарту Suite B для США.



*Во вкладке **Сертификаты** задаются параметры создаваемых ключей.*

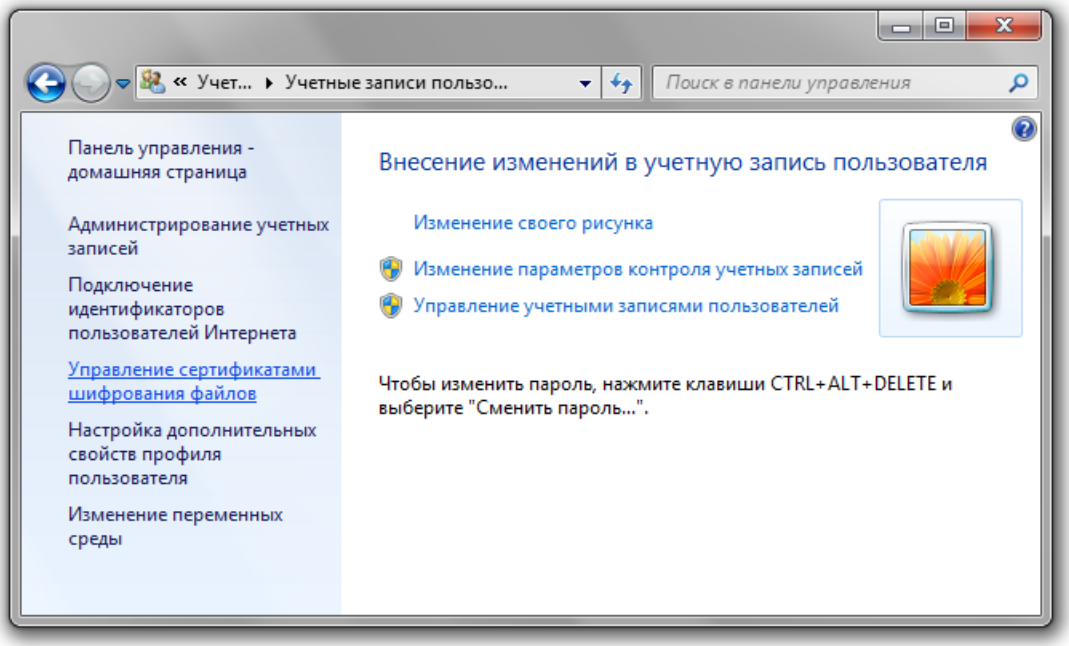


*Во вкладке **Кэш** настраиваются параметры управления кэширования ключей с карты. Ключи кэшируются для оптимизации производительности. В кэшированной памяти вместо самих закрытых ключей хранятся только дескрипторы контейнера ключа CryptoAPI.*

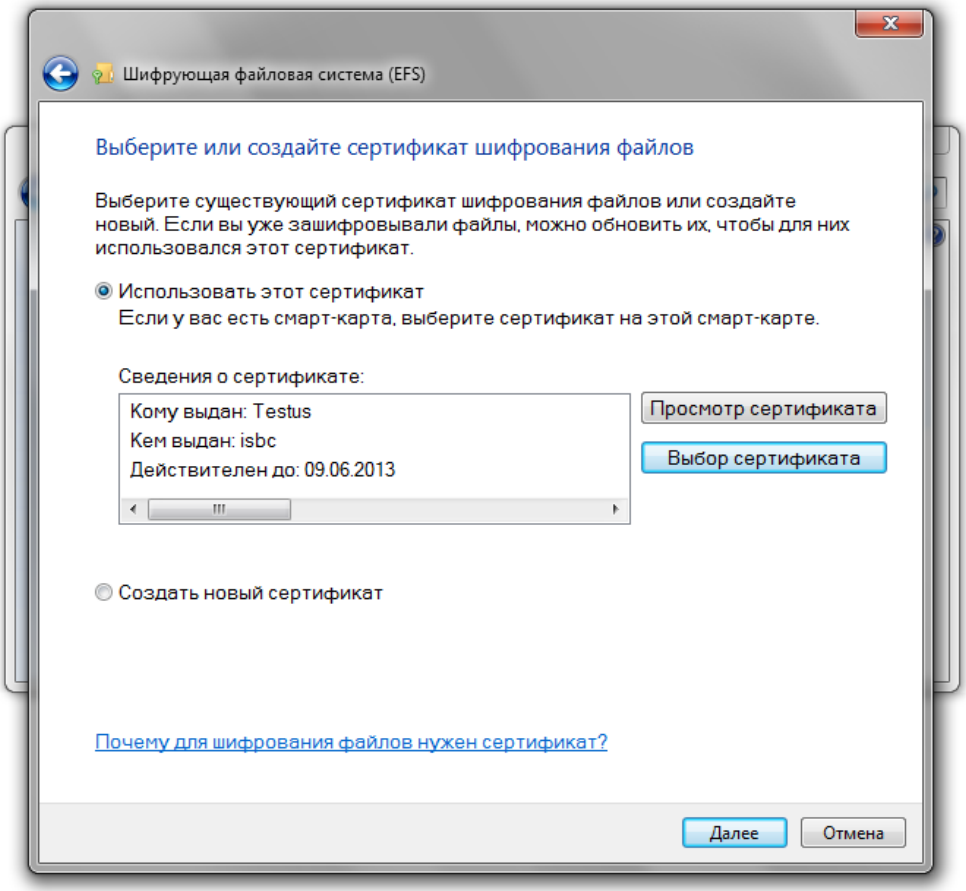


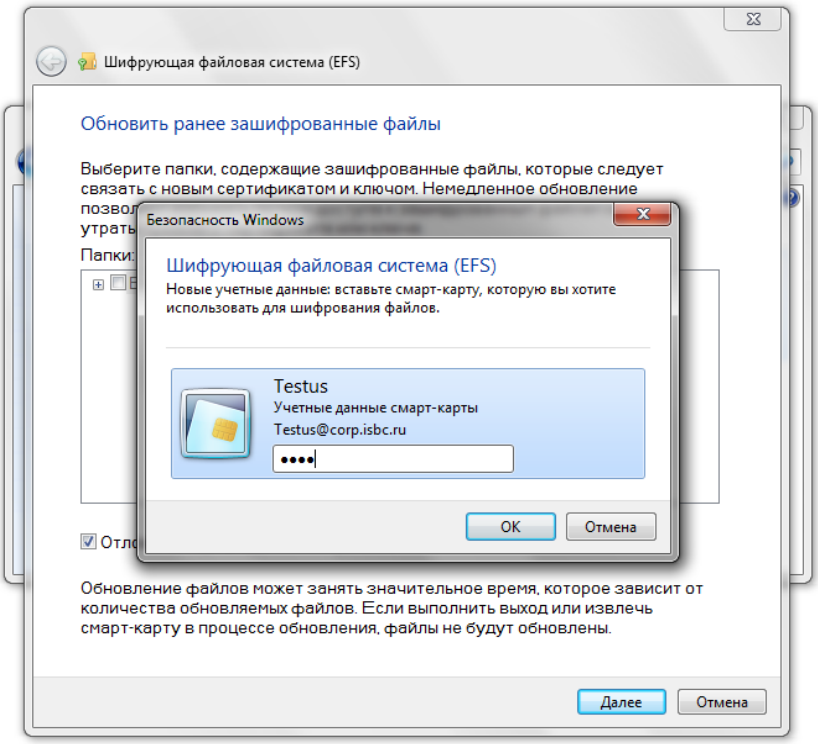
3.1 Создание сертификата на смарт-карте

Перейдите в панель управления. Выберите раздел ***Управление учетными записями пользователей****. В левой панели выберите* ***Управление сертификатами шифрования файлов****.*



Выберите один из имеющихся на карте сертификатов или создайте новый:

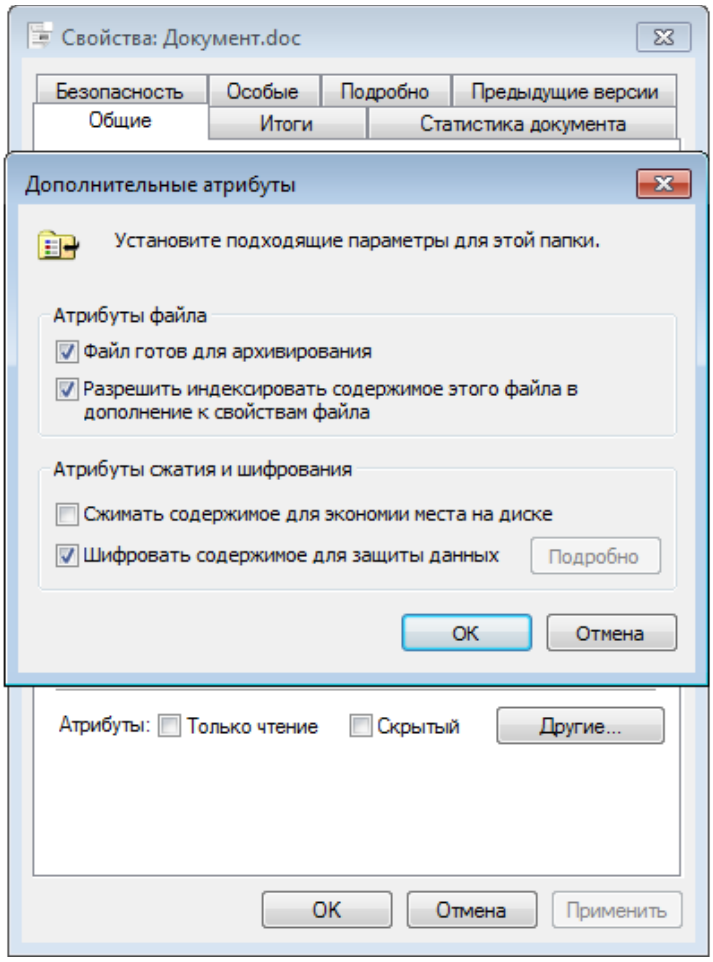

Шифрующая файловая система (EFS)
Выберите или создайте сертификат шифрования файлов
Выберите существующий сертификат шифрования файлов или создайте новый. Если вы уже зашифровывали файлы, можно обновить их, чтобы для них использовался этот сертификат.
Использовать этот сертификат
Если у вас есть смарт-карта, выберите сертификат на этой смарт-карте.
Сведения о сертификате:
Кому выдан: Testus
Кем выдан: isbc
Действителен до: 09.06.2013
Просмотр сертификата
Выбор сертификата
Создать новый сертификат
Почему для шифрования файлов нужен сертификат?
Далее
Отмена


Шифрующая файловая система (EFS)
Обновить ранее зашифрованные файлы
Выберите папки, содержащие зашифрованные файлы, которые следует связать с новым сертификатом и ключом. Немедленное обновление
Папки:
Безопасность Windows
Шифрующая файловая система (EFS)
Новые учетные данные: вставьте смарт-карту, которую вы хотите использовать для шифрования файлов.
Testus
Учетные данные смарт-карты
Testus@corp.isbc.ru
OK
Отмена
Обновление файлов может занять значительное время, которое зависит от количества обновляемых файлов. Если выполнить выход или извлечь смарт-карту в процессе обновления, файлы не будут обновлены.
Далее
Отмена

4. Шифрование папки или файла

4.1 Шифрование через свойства файла

1. *Щелкните правой кнопкой мыши папку или файл, которые требуется зашифровать, и щелкните **Свойства**.*
2. *Перейдите на вкладку **Общие** и щелкните **Дополнительно**.*



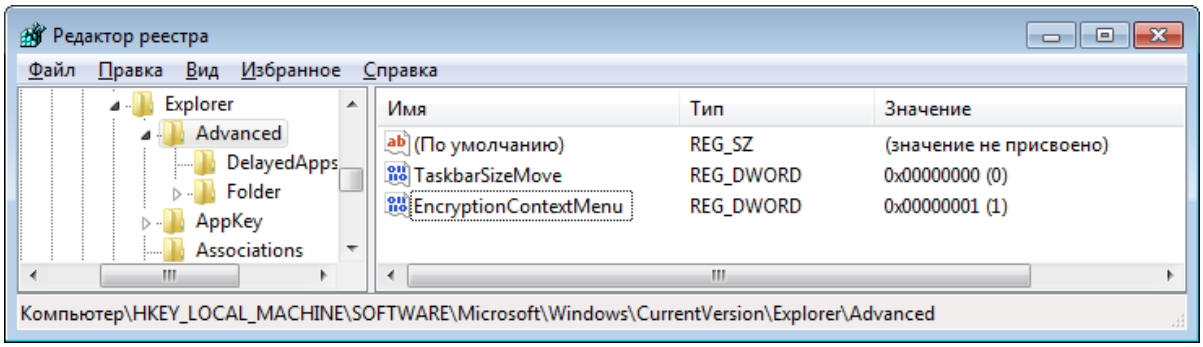
3. *Установите флажок **Шифровать** содержимое для защиты данных и нажмите **OK**. Нажмите **Применить** или **OK** в окне свойств файла.*
4. *Для расшифровки снимите флажок **Шифровать** содержимое для защиты данных и последовательно нажмите кнопку **OK** два раза.*

4.2 Шифрование через контекстное меню

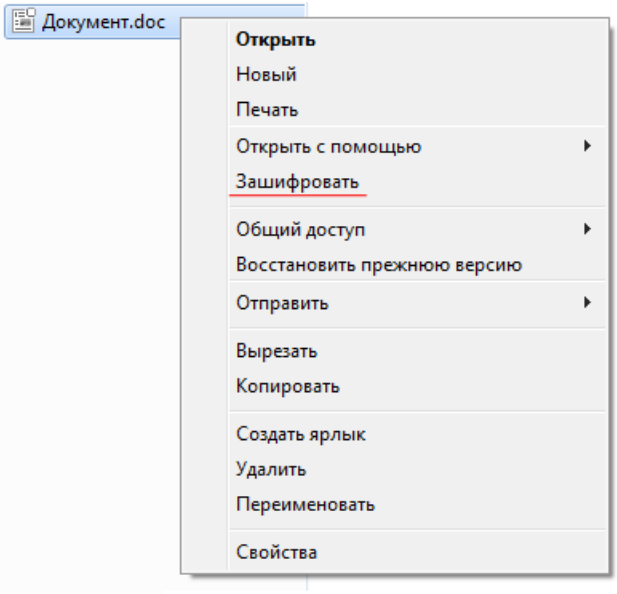
*Для удобства пользователей можно вывести команду **зашифровать/расшифровать файл** в контекстное меню. Для выполнения операции требуются права администратора.*

Откройте редактор реестра:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced

*Создайте новый параметр **DWORD** с именем **EncryptionContextMenu** и значением **1**.*



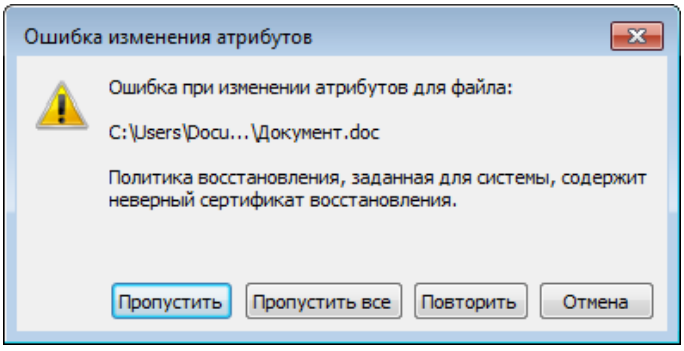
Теперь шифрование доступно напрямую из контекстного меню без необходимости заходить в свойства файла.



5. Возможные проблемы

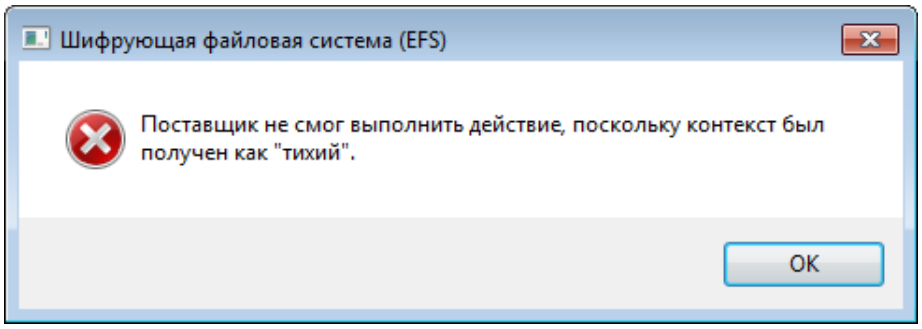
5.1 Неверный сертификат восстановления

Для полноценного использования EFS-шифрования потребуется создать сертификат восстановления. Агентом восстановления по умолчанию является первый администратор контроллера домена. Подробнее о сертификатах восстановления читайте на сайте Microsoft. (http://windows.microsoft.com/ru-RU/windows-vista/Create-a-recovery-certificate-for-encrypted-files).

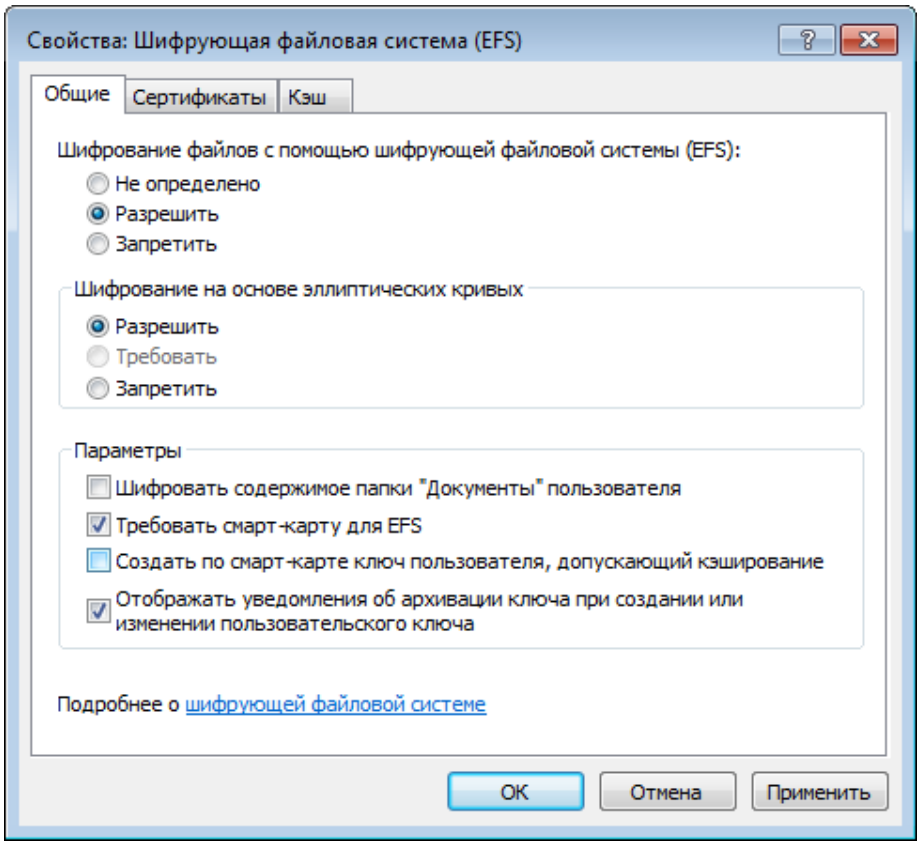


5.2 Поставщик не смог выполнить действие, поскольку контекст был получен как «тихий»

Если после ввода ПИН-кода появляется сообщение об ошибке:

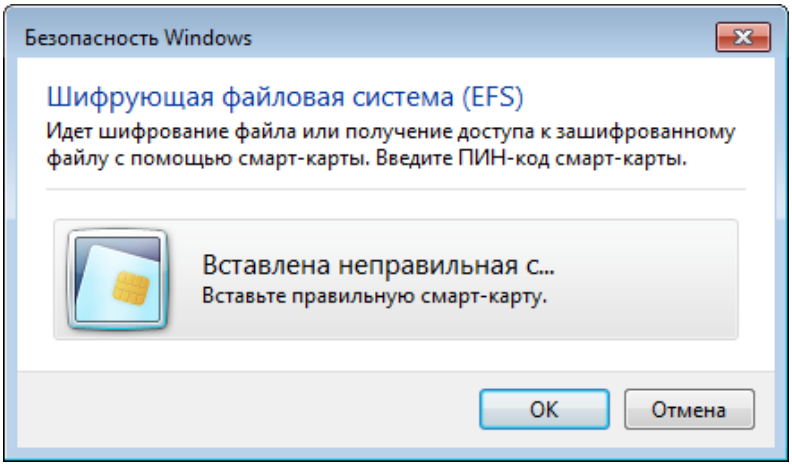


Откройте локальный редактор групповых политик (secpol.msc) или редактор групповых политики домена. Разверните узел ***Политики открытого ключа****, щелкните правой кнопкой мыши элемент* ***Шифрованная файловая система*** *и выберите пункт* ***Свойства****.*



Снимите галочку ***Создать по смарт-карте ключ пользователя, допускающий кэширование****.*

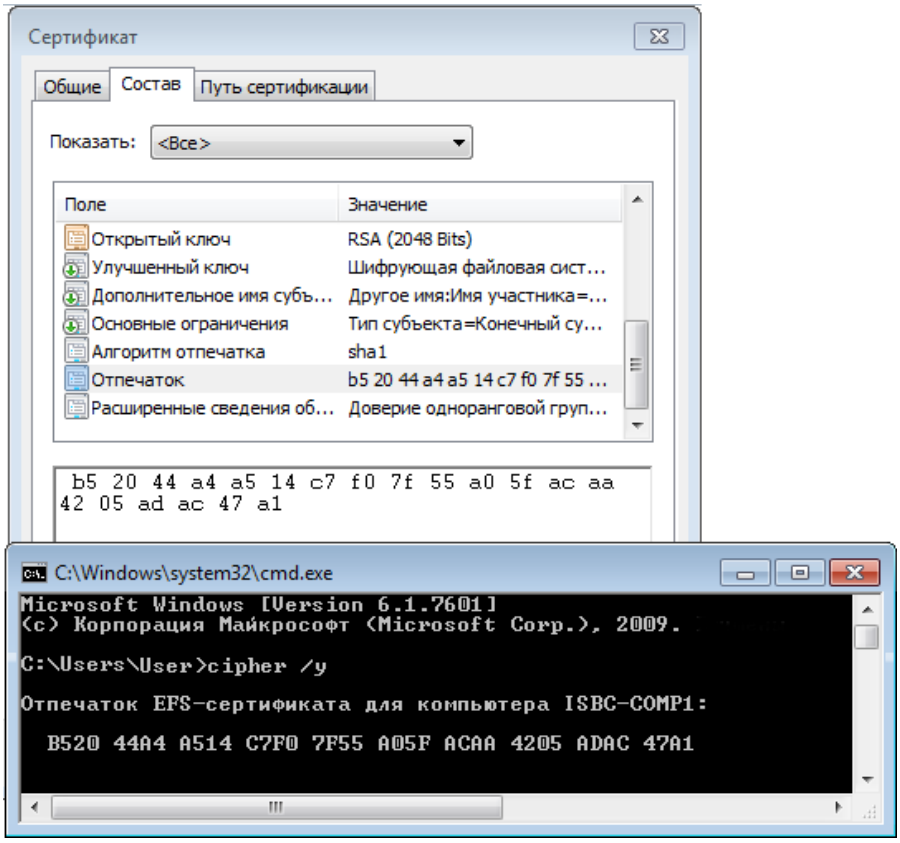
5.3 Вставлена неправильная смарт-карта



Убедиться, что сертификат на карте действительно является сертификатом, который будет использоваться для EFS, можно следующим образом:

Откройте отпечаток (fingerprint) сертификата, например, при помощи ESMART PKI Client.

*Откройте командную строку и введите **cipher /y**, чтобы вывести отпечаток текущего сертификата, установленного для EFS.*



Если отпечатки совпадают, сертификат на смарт-карте является сертификатом для EFS-шифрования. Если отпечатки отличаются, возможно, был запрошен новый сертификат или пользователь пытается использовать смарт-карту, на которой нет сертификата, подходящего для EFS.