

# 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	3
1.1	Преимущества EFS	3
1.2	Уязвимость EFS	3
2.	Подготовка к работе	3
3.	Настройка EFS	3
3.1	Создание сертификата на смарт-карте	6
4.	Шифрование папки или файла	8
4.1	Шифрование через свойства файла	8
4.2	Шифрование через контекстное меню	8
5.	Возможные проблемы	9
5.1	Неверный сертификат восстановления	9
5.2	Поставщик не смог выполнить действие, поскольку контекст был получен как «тихий» 1	0
5.3	Вставлена неправильная смарт-карта1	1



# 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.

🚡 Локальная политика безопасности			
Файл Действие Вид Справка			
<ul> <li>Параметры безопасности</li> <li>Политики учетных записей</li> <li>Локальные политики</li> <li>Брандмауэр Windows в режиме повышенной безопа</li> <li>Политики диспетчера списка сетей</li> <li>Политики открытого ключа</li> <li>Политики открытого ключа</li> <li>Шифрующая файловая система (EFS)</li> <li>Шифрование диска BitLocker</li> <li>Политики ограниченного использования программ</li> <li>Политики управления приложениями</li> <li>Политики IP-безопасности на "Локальный компьют</li> <li>Конфигурация расширенной политики аудита</li> </ul>	Кому выдан Кем выдан Нет элементов для отображения в этом виде. Добавить агент восстановления данных Создать агент восстановления данных Создать расстановления данных Создать агент восстановления данных Создать в создать агент восстановления данных Создать восстановления данных Создать в создать в со		
< >	< •		
Открытие окна свойств выбранного объекта.			

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.



Свойства: Шифрующая файловая система (EFS)	3				
Общие Сертификаты Кэш					
Шифрование файлов с помощью шифрующей файловой системы (EFS):					
О Не определено					
• Разрешить					
Запретить					
Шифрование на основе эллиптических кривых					
Разрешить					
🔘 Требовать					
Запретить					
Параметры Шифровать содержимое папки "Документы" пользователя Пребовать смарт-карту для EFS					
Создать по смарт-карте ключ пользователя, допускающий кэширование					
Отображать уведомления об архивации ключа при создании или изменении пользовательского ключа					
Подробнее о шифрующей файловой системе					
ОК Отмена Применить					

Во вкладке Сертификаты задаются параметры создаваемых ключей.

Свойства: Шифрующая файловая система (EFS)				
Общие Сертификаты Кэш				
Шаблон EFS для автоматических запросов сертификатов: Базовое шифрование EFS Обзор				
Самозаверяющие сертификаты				
Разрешить EFS создавать самозаверяющие сертификаты, если центр сертификации недоступен				
Размер ключа для самозаверяющих сертификатов RSA:				
2048  Размер ключа для самозаверяющих сертификатов шифрования на эллиптических кривых:				
256 🔻				
Дополнительные сведения о <u>сертификатах EFS</u>				
ОК Отмена Применить				

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.

Свойства: Шифрующая файловая система (EFS)		
Общие Сертификаты Кэш		
Очищать кэш ключей шифрования в следующих случаях:		
🔽 По истечении времени хранения кэша		
Предельное время хранения кэша:		
480 минут		
🔽 При блокировании рабочей станции пользователем		
Для очищения кэша необходимо извлечь смарт-карты из устройства чтения смарт-карт.		
Подробнее о <u>кэшировании EFS</u>		
ОК Отмена Применить		

#### 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:



ſ		η		
	😋 🕺 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.			
<ul> <li>Использовать этот сертификат</li> <li>Если у вас есть смарт-карта, выберите сертификат на этой смарт-карте.</li> </ul>				
	Сведения о сертификате:	I		
	Кому выдан: Testus			
	Действителен до: 09.06.2013 Выбор сертификата	I		
	4	I		
	Создать новый сертификат			
	Почему для шифрования файлов нужен сертификат?			
	Далее Отмена			

Обнови	іть ранее зашифрованные файлы
Выберит	ге папки, содержащие зашифрованные файлы, которые следует
связать	с новым сертификатом и ключом. Немедленное обновление
позвол утрать Папки:	Безопасность Windows           Шифрующая файловая система (EFS)           Новые учетные данные: вставьте смарт-карту, которую вы хотите использовать для шифрования файлов.           Теstus           Учетные данные смарт-карты           Testus@corp.isbc.ru           ••••
☑ Отла	ОК Отмена
Обновла	ение файлов может занять значительное время, которое зависит от
количес	тва обновляемых файлов. Если выполнить выход или извлечь

## 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.

📮 Свойства: Документ.doc 🔀				
Безопасность         Особые         Подробно         Предыдущие версии           Общие         Итоги         Статистика документа				
Дополнительные атрибуты				
Установите подходящие параметры для этой папки.				
Атрибуты файла				
📝 Файл готов для архивирования				
Разрешить индексировать содержимое этого файла в дополнение к свойствам файла				
Атрибуты сжатия и шифрования				
🔲 Сжимать содержимое для экономии места на диске				
Шифровать содержимое для защиты данных Подробно				
ОК Отмена				
Атрибуты: 🔲 Только чтение 🔲 Скрытый Другие				
ОК Отмена Применить				

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

Документ.doc	Открыть	
	Новый	
	Печать	
	Открыть с помощью	•
	Зашифровать	
	Общий доступ	•
	Восстановить прежнюю версию	
	Отправить	+
	Вырезать	
	Копировать	
	Создать ярлык	
	Удалить	
	Переименовать	
	Свойства	

### 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. (<u>http://windows.microsoft.com/ru-RU/windows-vista/Create-a-recovery-certificate-for-encrypted-files</u>).





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

Если после ввода ПИН-кода появляется сообщение об ошибке:

💷 Шифрующая файловая система (EFS)	×
Поставщик не смог выполнить действие, поскольку контекс получен как "тихий".	т был
	ОК

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.

Свойства: Шифрующая файловая система (EFS)				
Общие Сертификаты Кэш				
Шифрование файлов с помощью шифрующей файловой системы (EFS):				
🔘 Не определено				
• Разрешить				
Запретить				
Шифрование на основе эллиптических кривых				
Разрешить				
🔘 Требовать				
Запретить				
Параметры Шифровать содержимое папки "Документы" пользователя Tpeбовать смарт-карту для EFS Coздать по смарт-карте ключ пользователя, допускающий кэширование Отображать уведомления об архивации ключа при создании или изменении пользовательского ключа				
Подробнее о <u>шифрующей файловой системе</u>				
ОК Отмена Применить				

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.

Сертификат		X				
Общие Состав Путь сертификации						
Показать: <все>	▼					
Поле	Значение	*				
Сткрытый ключ Сткрытый ключ Сполнительное имя субъ Соновные ограничения Алгоритм отпечатка Отпечаток Расширенные сведения об b5 20 44 a4 a5 14 c7 42 05 ad ac 47 a1	RSA (2048 Bits) Шифрующая файловая сист Другое имя:Имя участника= Тип субъекта=Конечный су sha1 b5 20 44 a4 a5 14 c7 f0 7f 55 Доверие одноранговой груп f0 7f 55 a0 5f ac aa	E				
C:\Windows\system32\cmd.exe		- • <b>·</b>				
Microsoft Windows [Version 6.1.7601] (с) Корпорация Майкрософт (Microsoft Corp.), 2009.						
С:\Users\User>cipher /у Отпечаток EFS-сертификата для компьютера ISBC-COMP1: B520 44A4 A514 C7F0 7F55 A05F ACAA 4205 ADAC 47A1						
J • III		<u>ایا</u> ا				

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