УДК 004.056.5

магистр А.А. Филимонов
ГВУЗ «Национальный горный университет»

РАЗВЕРТЫВАНИЕ ФАЙЛОВОЙ СИСТЕМЫ EFS

В данной статье описано развертывание файловой системы EFS с целью реализации требований к защищенности обрабатываемой информации.

EFS (Encrypting File System) - это шифрованная файловая система которая является частью системы NTFS. Шифрованная файловая система позволяет пользователям хранить данные на диске в зашифрованном виде [1].

Зашифрованный одним пользователем файл не может быть открыт другим пользователем, если ему не назначены соответствующие разрешения [2].

EFS имеет два уровня настройки. Первый уровень установлен на компьютерном уровне, который определяет, будет ли поддерживаться эта файловая система, и будет ли она доступна. Второй уровень – это уровень папок и файлов, этот уровень выполняет шифрование данных. Windows 2000 (Server и Professional), Windows XP Professional, Windows Server 2003, Windows Vista и Windows Server 2008 все поддерживают шифрование данных, расположенных на компьютере [3].

Центр сертификации системы Windows Server 2008 поставляется с предоставляемым по умолчанию набором шаблонов сертификатов, включая шаблон Basic EFSBasic EFS (Базовое шифрование EFS). Однако этот шаблон не поддерживает архивирование ключей. Поэтому прежде чем делать его доступным в своем центре сертификации, нужно создать копию этого шаблона для создания нового шаблона версии 2. В этом новом шаблоне на вкладке Request HandlingRequest Handling (Обработка запросов) необходимо установить флажок архивирования ключей шифрования пользователей. Прежде чем включать этот параметр, необходимо правильно настроить архивирование ключей в центре сертификации. Также следует заместить

этим шаблоном шаблонBasic EFS Basic EFS (Базовое шифрование EFS), чтобы гарантировать использование клиентами этой новой версии.

Так как компонент EFS в системе Windows автоматически запрашивает сертификат при первом использовании системы EFS, обычно нет необходимости разрешать пользователям автоматическую подачу заявок для шаблона EFS. Не рекомендуется включать автоматическую подачу этих заявок, если нет уверенности в том, что все автоматически подающие заявки пользователи будут использовать систему EFS.

Архивирование ключей обеспечивает администраторам центров сертификации возможность восстанавливать ключи шифрования для пользователей. С архивированием и восстановлением ключей следует обращаться очень небольшому кругу заслуживающих доверия сотрудников службы безопасности. Так как операция восстановления ключей затрагивает конфиденциальность, в качестве основного механизма восстановления доступа к зашифрованным с помощью системы EFS данным важно направить группе администрирования центра сертификации четко определенный процесс передачи запросов о восстановлении по инстанциям. Процесс восстановления должен инициироваться только после тщательной проверки таких запросов. Затем после фактического восстановления ключа он должен предоставляться пользователю безопасным методом (не по электронной почте), так как восстановленный ключ обеспечивает доступ ко всем защищенным с помощью системы EFS данным пользователя.

Определив, на каких компьютерах система EFS используется, а на каких не используется, нужно отключить автономный режим системы EFS на всех компьютерах, где эта система в настоящее время не применяется. Этот этап процесса развертывания весьма важен, поскольку проще активировать и правильно настроить систему EFS впервые, чем проводить миграцию пользователей, работающих с самозаверяющими сертификатами. Приступать к его осуществлению нужно только тогда, когда перечень лиц, использующих систему EFS, станет точно известен [4].

Система EFS предоставляет в распоряжение администраторов Windows метод защиты информации, характеризуемый высоким уровнем безопасности. Система EFS отличается масштабируемостью, управляемостью и обеспечивает гибкие механизмы восстановления данных.

Перечень литературы:

1. The Encrypting File System, Roberta Bragg [Электронный ресурс] - режим доступа: http://technet.microsoft.com/en-us/library/cc700811.aspx

2. EFS - Encrypting File System [Электронный ресурс] - режим доступа: http://www.oszone.net/1295/#full_page_top

3. Контроль шифрованной файловой системы с помощью групповой политики [Электронный ресурс] - режим доступа: http://faqman.ru/windows-security/kontrol-dostupa-i-shifrovanie/kontrol-shifrovannoj-fajlovoj-sistemy-encrypting-file-system-%E2%80%93-efs-s-pomoshhyu-gruppovoj-politiki.html

4. В поисках безопасности. Развертывание файловой системы EFS [Электронный ресурс] - режим доступа: http://www.winblog.ru/2007/04/06/06040701.html