

BitLocker в Windows Server 2008 и Windows Vista SP1: архитектура и варианты применения

Александр Шаповал

Содержание

- Назначение и особенности технологии BitLocker
- Архитектура и принципы работы
- Настройка и восстановление системы

Назначение и особенности

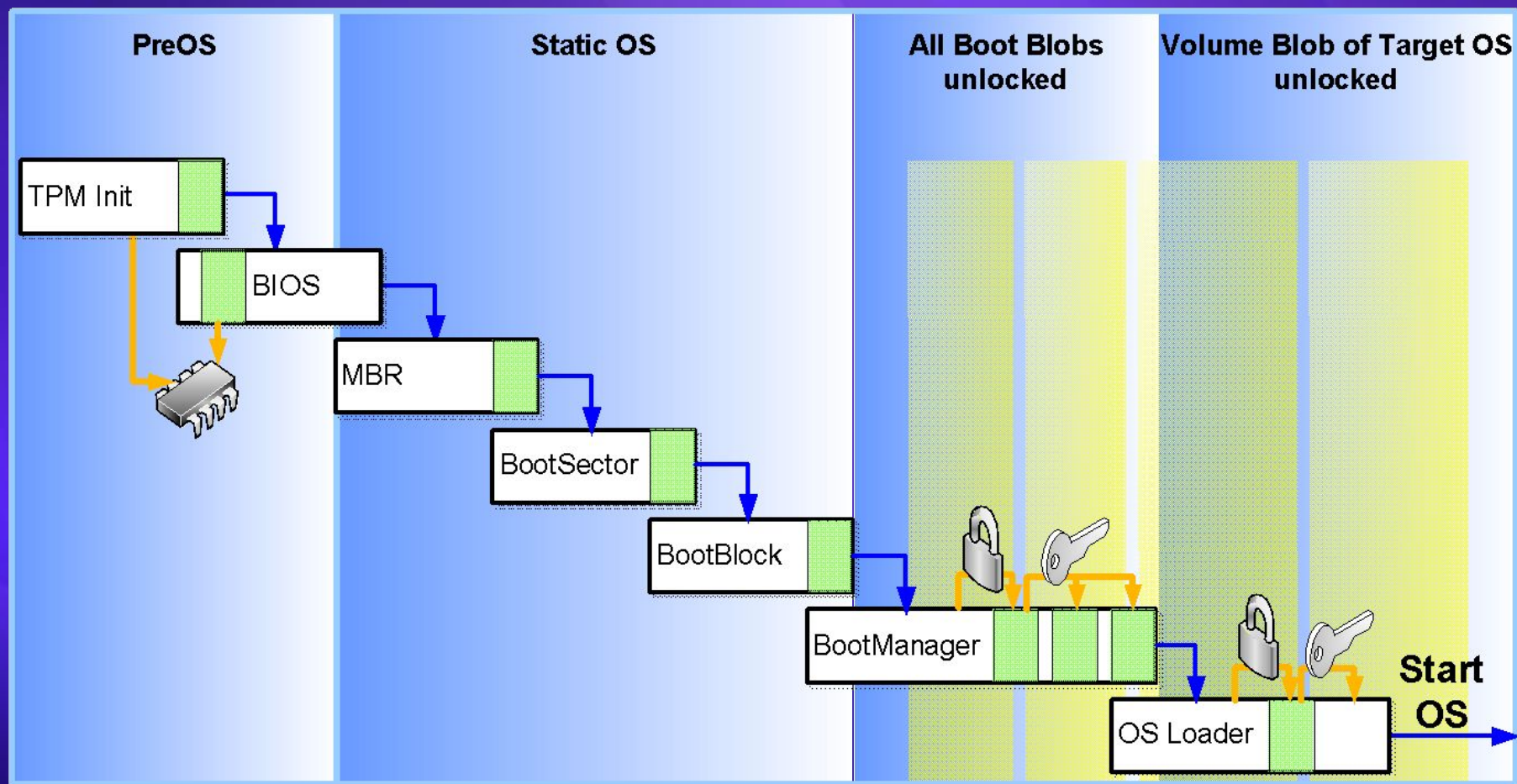
- Предотвращает несанкционированный доступ к данным
- Обеспечивает полное шифрование всего тома, включая:
 - Файл подкачки, временные файлы и пр.
- Использует Trusted Platform Module (TPM) v1.2 для хранения ключа и проверки целостности системы на этапе загрузки
- Поддерживает защиту нескольких томов/устройств
 - Windows Vista SP1, Windows Server 2008

Trusted Platform Module

- Аппаратный модуль (чип) для выполнения криптографических операций
 - Создание, хранение, управление ключами
 - Шифрование, цифровая подпись
 - RSA, SHA-1, RNG
- Проверяет целостность критически важных компонент системы на этапе загрузки



TPM и загрузка ОС



Архитектура TPM

PCR[15]
PCR[14]
PCR[13]
PCR[12]
PCR[11]
PCR[10]
PCR[9]
PCR[8]
PCR[7]
PCR[6]
PCR[5]
PCR[4]
PCR[3]
PCR[2]
PCR[1]
PCR[0]

- Регистры хранят хэши различных компонент системы
- Перед выполнением любой код сначала хэшируется с помощью SHA-1, затем результат сверяется со значением соответствующего регистра
- Назначение регистров
 - PCR[0], PCR[1] – BIOS и расширения
 - PCR[2], PCR[3] – дополнительные носители
 - PCR[4] – Master Boot Record (MBR)
 - PCR[5] – Partition Table
 - PCR[8] – Boot Sector
 - PCR[9] – Boot Block
 - PCR[10] – Boot Manager
 - PCR[11] – ключ BitLocker

Архитектура TPM

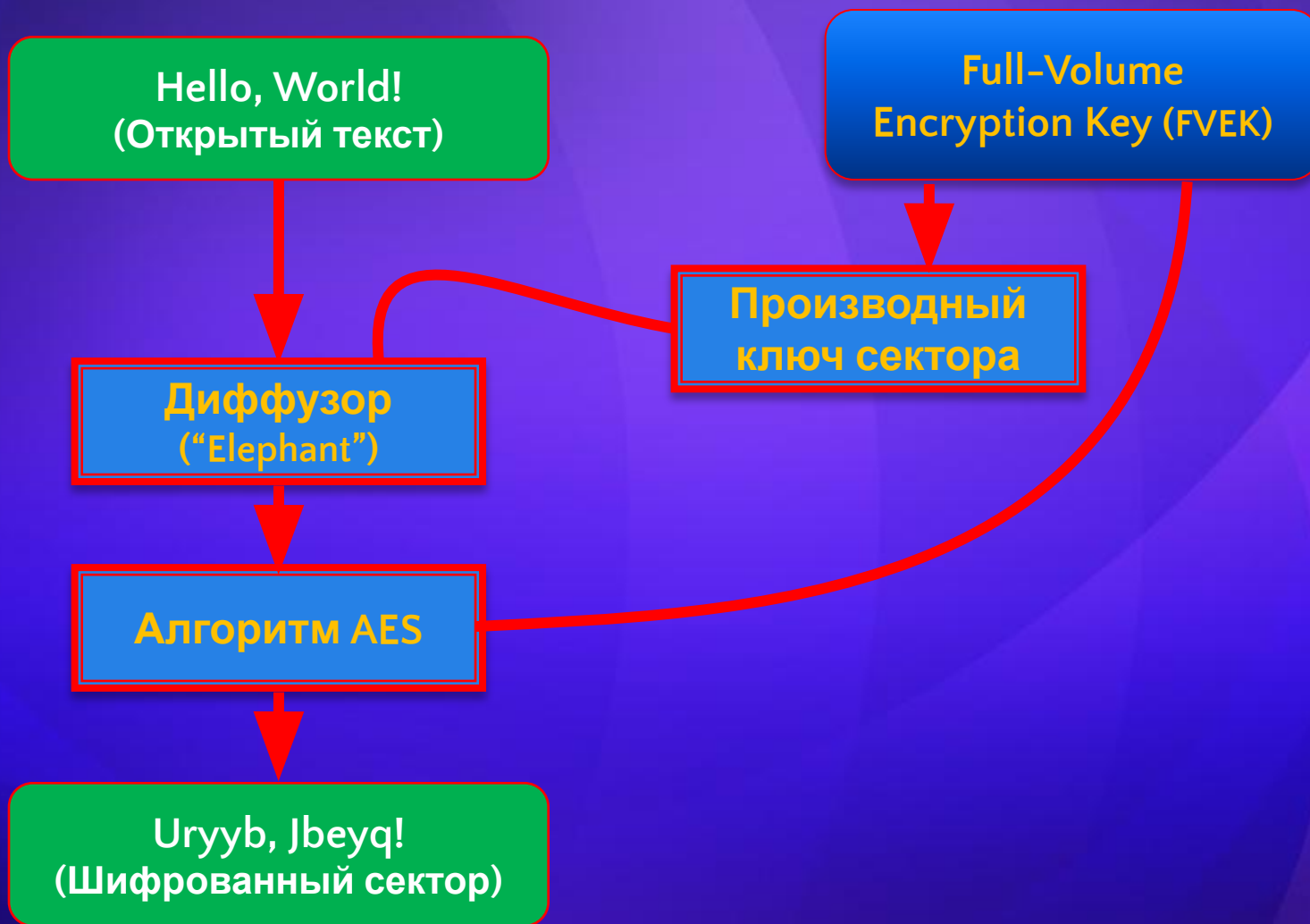
PCR[15]
PCR[14]
PCR[13]
PCR[12]
PCR[11]
PCR[10]
PCR[9]
PCR[8]
PCR[7]
PCR[6]
PCR[5]
PCR[4]
PCR[3]
PCR[2]
PCR[1]
PCR[0]

- Любые дополнительные загрузчики должны запускаться с зашифрованного тома
- По умолчанию BitLocker использует регистры: 4,8,9,10,11
- Включение дополнительных регистров влияет на возможность конфигурации системы
- Регистры 2 и 3
 - Любые изменения, включая добавление устройств для чтения смарт-карт или USB-устройств
- Регистры 0 и 1
 - Обновление BIOS

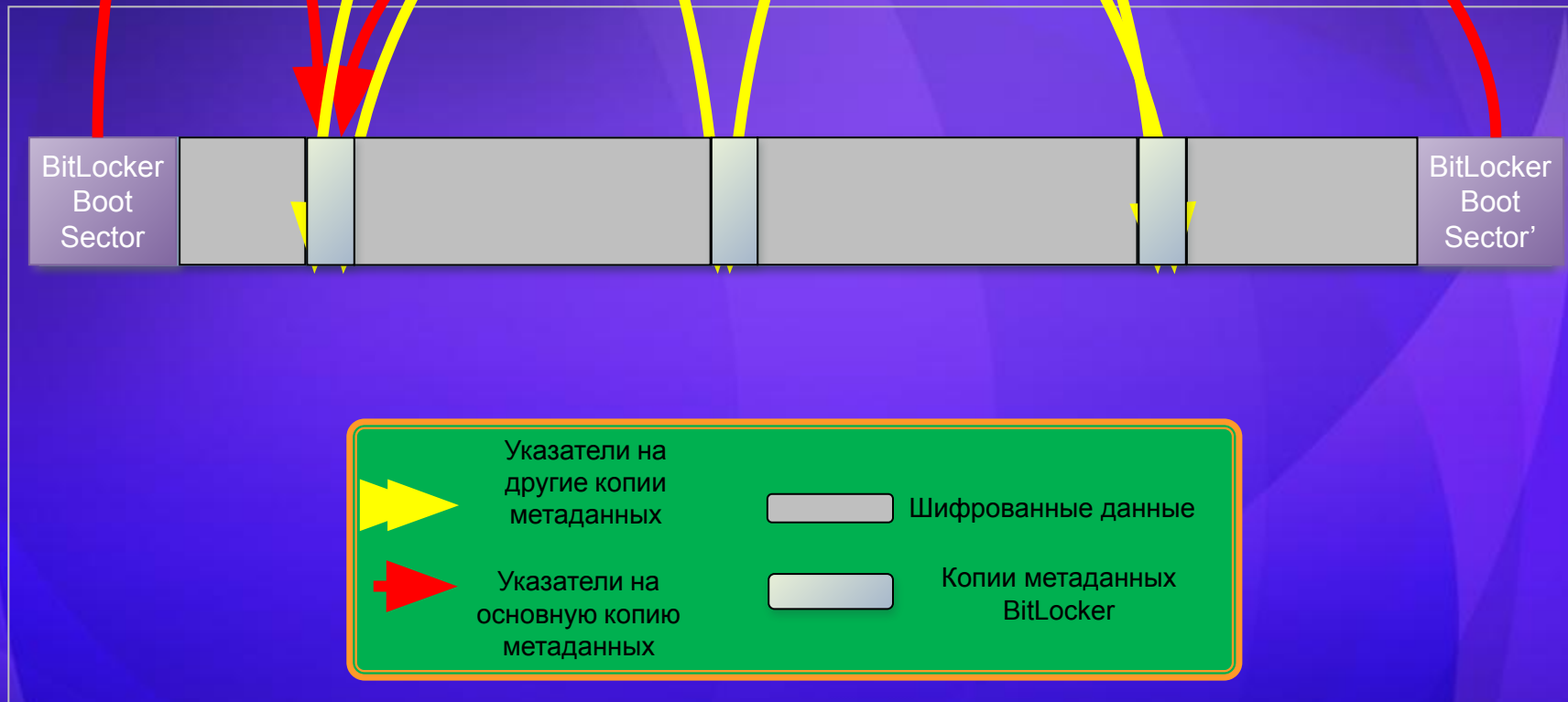
Шифрование тома

- Создается ключ, Full-Volume Encryption Key (FVEK), с помощью которого производится шифрование всего тома
 - Разовая длительная операция
 - В дальнейшем нагрузка на систему минимальна
- FVEK шифруется с помощью Volume Master Key (VMK)
- VMK защищается способом, определенным настройками и режимом работы системы

Шифрование тома



Структура тома BitLocker



В полях метаданных в том числе хранятся FVEK и VMK

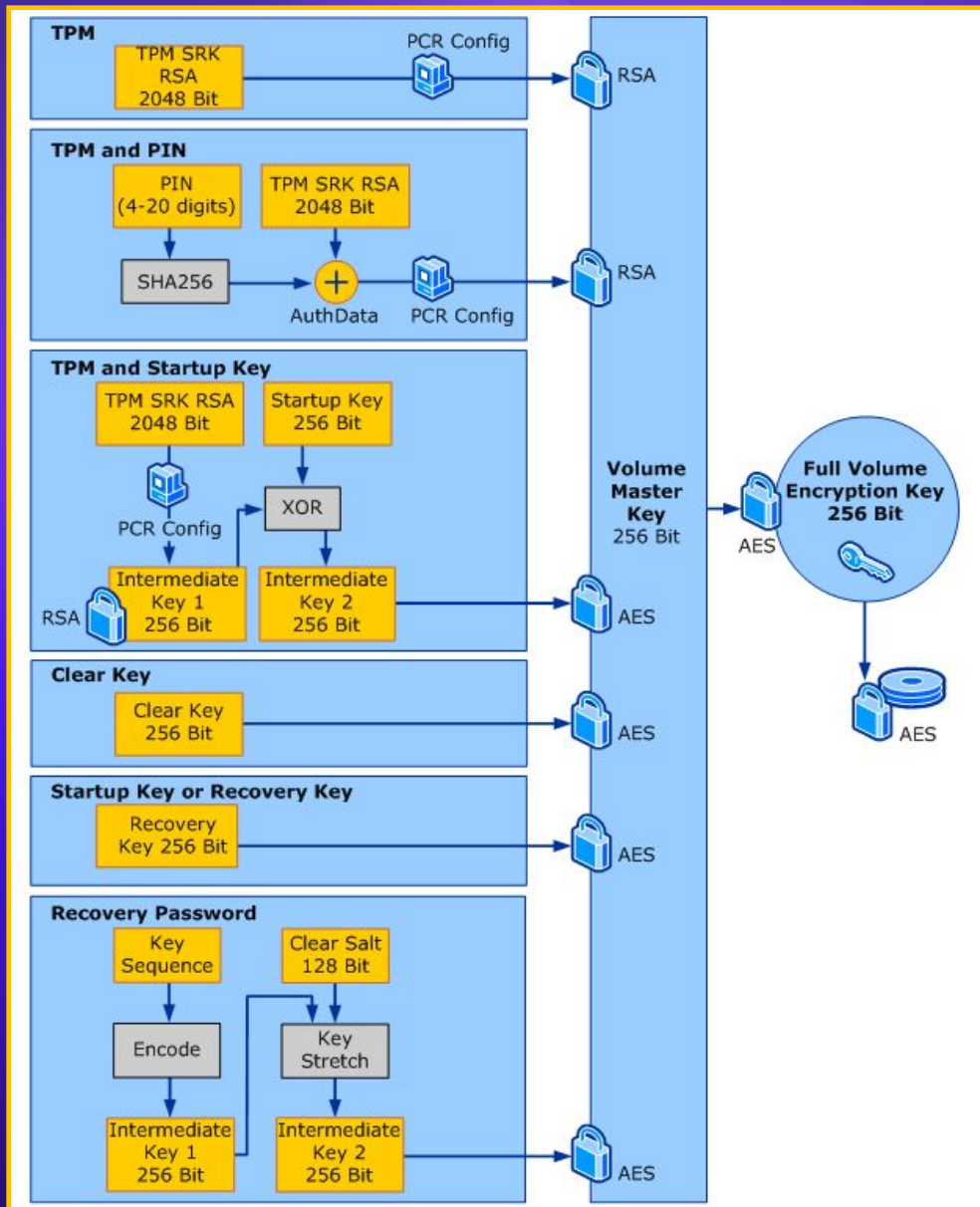
Режимы работы

- Временное отключение BitLocker
 - Изменение конфигурации системы
 - Перенос жесткого диска, обновление BIOS и пр.
 - Том остается зашифрованным
 - Незашифрованный ключ (Clear Key) для доступа к VMK
- Аутентификация
 - Только TPM
 - TPM + ключ запуска (Startup Key)
 - TPM + PIN
 - Только ключ запуска
 - Проверка целостности системы при загрузке отсутствует!
- Восстановление
 - Пароль восстановления (Recovery Password)
 - Ключ восстановления (Recovery Key)

Поиск ключей при старте

- Clear key
- Recovery Key или Startup Key
- TPM
- TPM + Startup Key
- TPM + PIN
- Recovery Password
- Recovery Key

Защита ключей



Системные требования

- BIOS должен поддерживать USB-устройства
- Наличие в системе TPM v1.2
 - Если нет TPM, обязательно использование ключа запуска на съемном USB-устройстве
- Операционная система
 - Windows Vista Ultimate
 - Windows Vista Enterprise
 - Windows Server 2008
- Жесткий диск
 - Минимум два раздела
 - Раздел с ОС (Boot Volume), NTFS
 - Активный раздел загрузки (System Volume), NTFS, ≥ 1.5 ГБ

Шифрование нескольких томов

- Доступно в Windows Vista SP1 и Windows Server 2008
- Поддерживается произвольное количество любых томов за исключением:
 - Активного раздела
 - Раздела запущенной в настоящий момент ОС
- Возможно автоматическое монтирование томов с данными
 - VMK каждого тома защищается незашифрованным ключом (auto-unlock key, AUK)
 - AUK хранятся в реестре (на зашифрованном томе)
 - Том ОС должен быть зашифрован

Настройки BitLocker

- Панель управления
 - Инициализация BitLocker
 - Управление ключами
- Сценарии WMI
 - Manage-bde.wsf
- Групповые политики

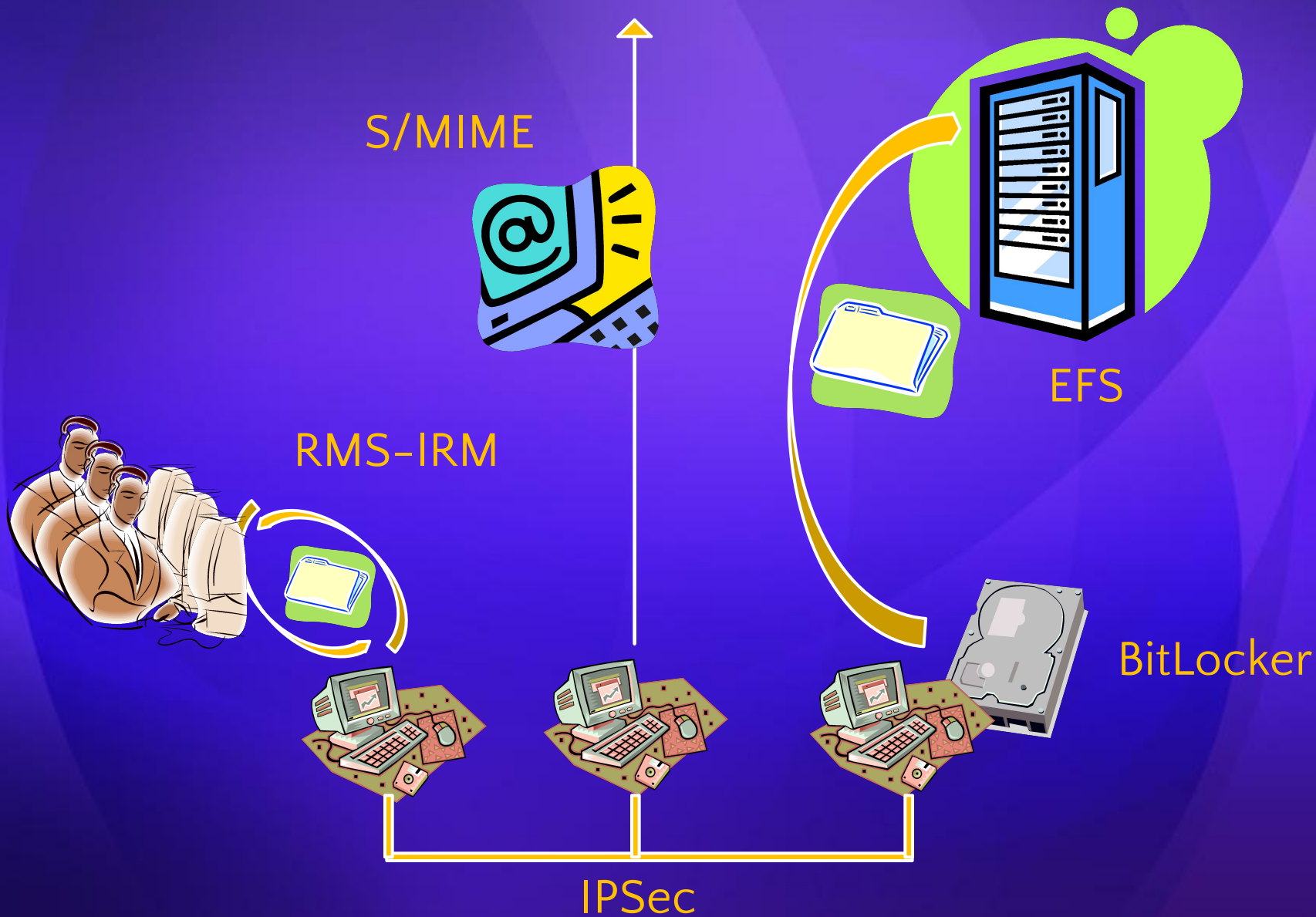
demo

Настройка
технологии BitLocker

Восстановление системы

- Когда может потребоваться восстановление:
 - Замена материнской платы
 - Обновление BIOS
 - Перенос жесткого диска на другой компьютер
 - Пользователь забыл PIN-код
 - ...
- При инициализации требуется включить как минимум одну опцию восстановления
 - Данные восстановления можно сохранить в AD
- Опции восстановления
 - Пароль восстановления (Recovery Password)
 - 48 цифр, при восстановлении набираются с помощью функциональных клавиш (F0 – F9)
 - Ключ восстановления (Recovery Key)
 - Сохраняется на USB-устройстве

Защита данных в Windows



Дополнительная информация

- [BitLocker FAQ](#)
- [Windows BitLocker Drive Encryption step-by-step guide](#)
- [Windows Vista Trusted Platform Module Services step-by-step guide](#)
- [Windows BitLocker Drive Encryption Design and Deployment Guides](#)
- [Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information](#)
- [Deploying BitLocker with the Data Encryption Toolkit for Mobile PCs](#)
- [BitLocker Drive Encryption Technical Overview](#)
- [Implementing BitLocker on Servers](#)

Вопросы

- <http://blogs.technet.com/ashapo>
- <http://www.microsoft.com/Rus/events>