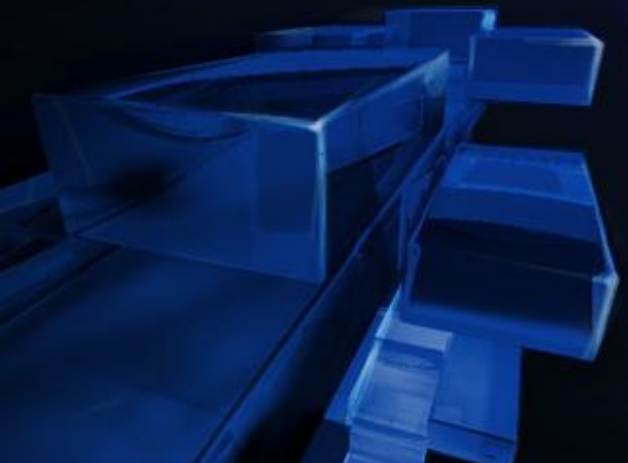
Microsoft Платформа 2008

Технологии защиты корпоративных данных в Windows Server 2008 и Windows Vista

Александр Шаповал



Содержание

- Краткий обзор технологий защиты
- BitLocker
- Active Directory Rights Management Services

Содержание

- Краткий обзор технологий защиты
- BitLocker
- Active Directory Rights Management Services

Новые возможности

Безопасность

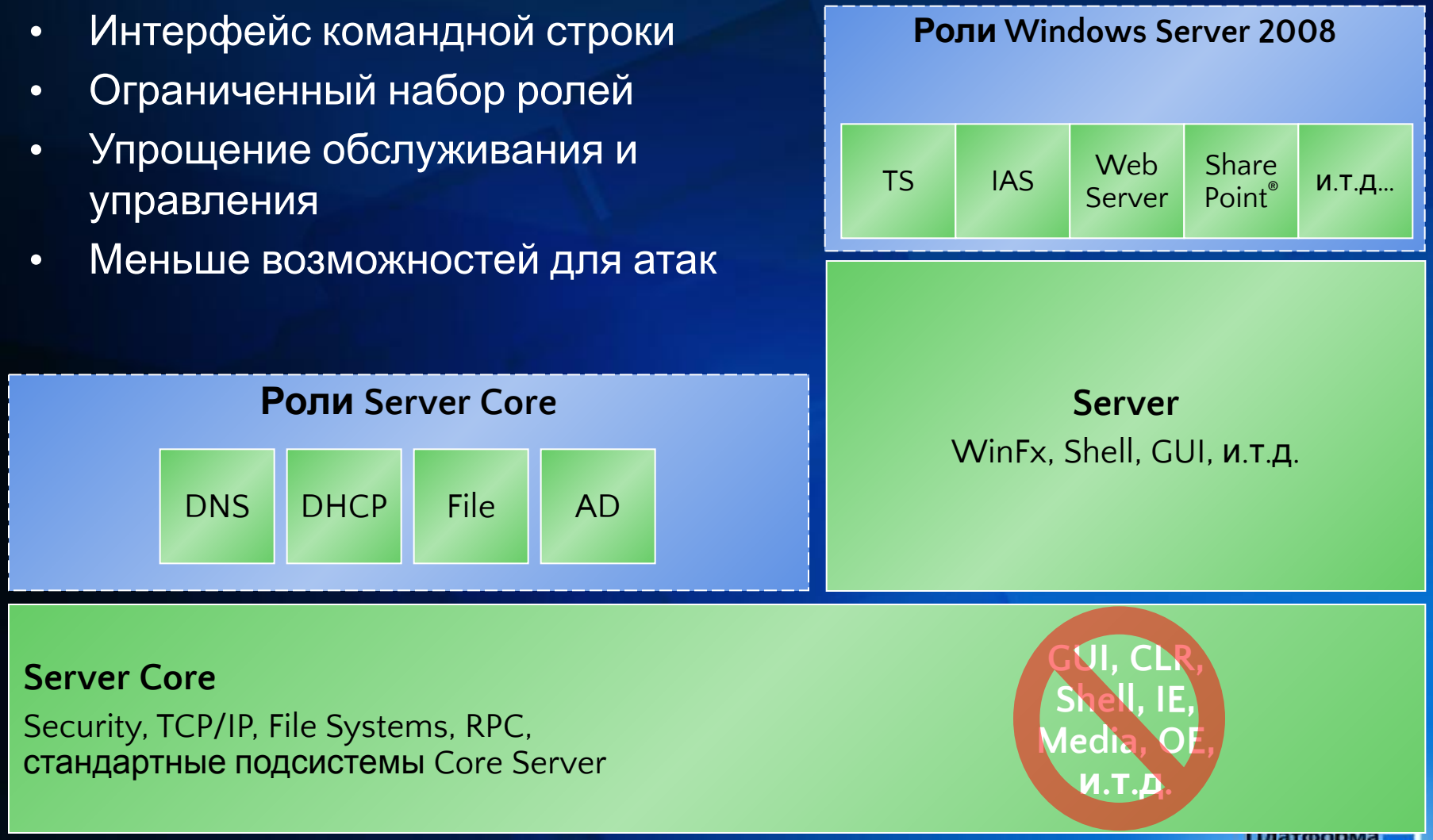
- Процесс разработки
- Безопасная загрузка и защита при установке
- Целостность кода
- Повышение защищенности служб Windows
- Межсетевой экран для входящего и исходящего трафика
- Диспетчер перезапуска

Соответствие политикам

- Улучшенный аудит
- Network Access Protection
- Переадресация событий
- Управление сетью на основе политик
- Изоляция сервера и домена
- Управление установкой съемных устройств
- Службы управления правами Active Directory

Server Core

- Минимальная инсталляция
- Интерфейс командной строки
- Ограниченный набор ролей
- Упрощение обслуживания и управления
- Меньше возможностей для атак



Платформа 2008

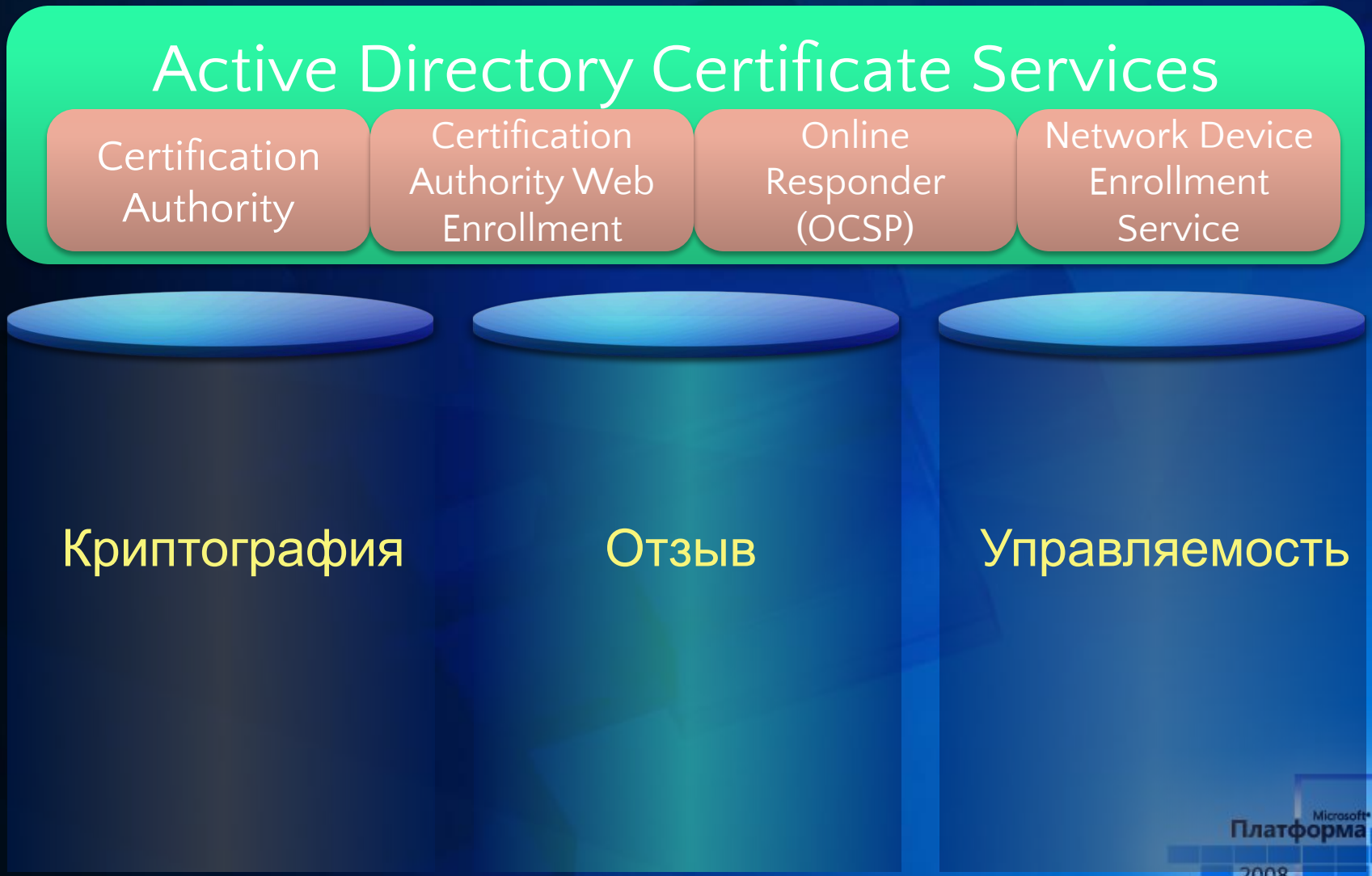
Network Access Protection

Microsoft Платформа 2008

Read Only Domain Controller

- Основные возможности
  - Копия базы AD в режиме «только чтение»
  - DNS в режиме «только чтение»
  - Разделение административных ролей
  - Односторонняя репликация
  - Кэширование параметров учетных записей

Расширения служб сертификации



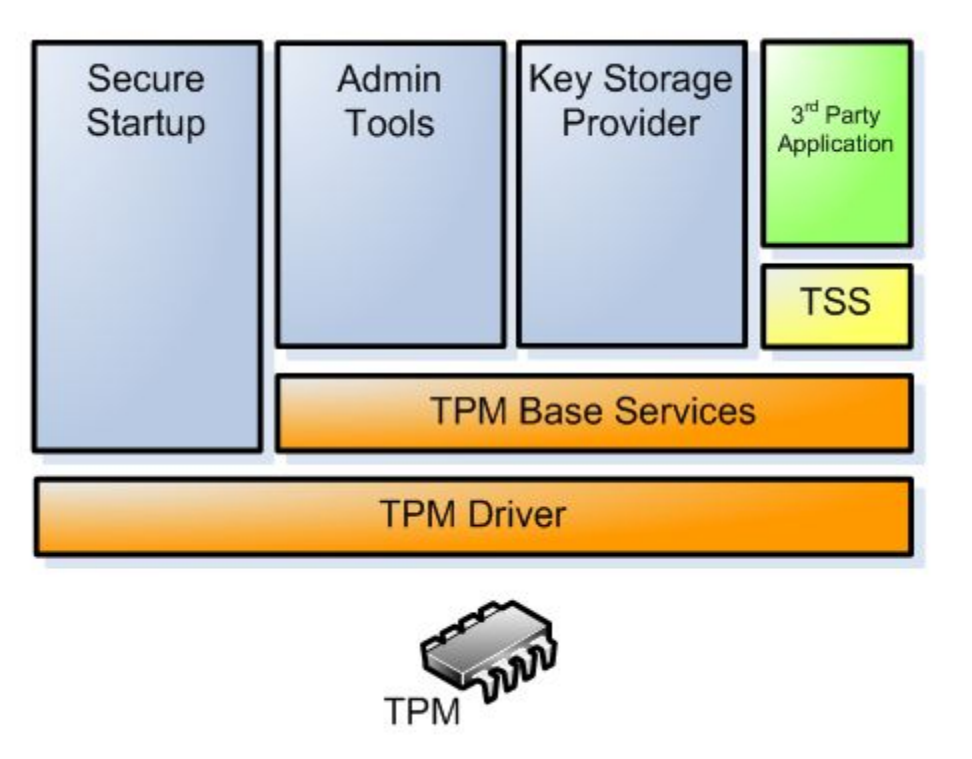
Содержание

- Краткий обзор технологий защиты
- BitLocker
- Active Directory Rights Management Services

Шифрование дисков с помощью BitLocker™

- Защита от неавторизованного доступа к данным
- Защита от физической кражи систем
- Безопасный старт системы
- Хранение ключей в TPM или на USB-носителе

Архитектура TPM



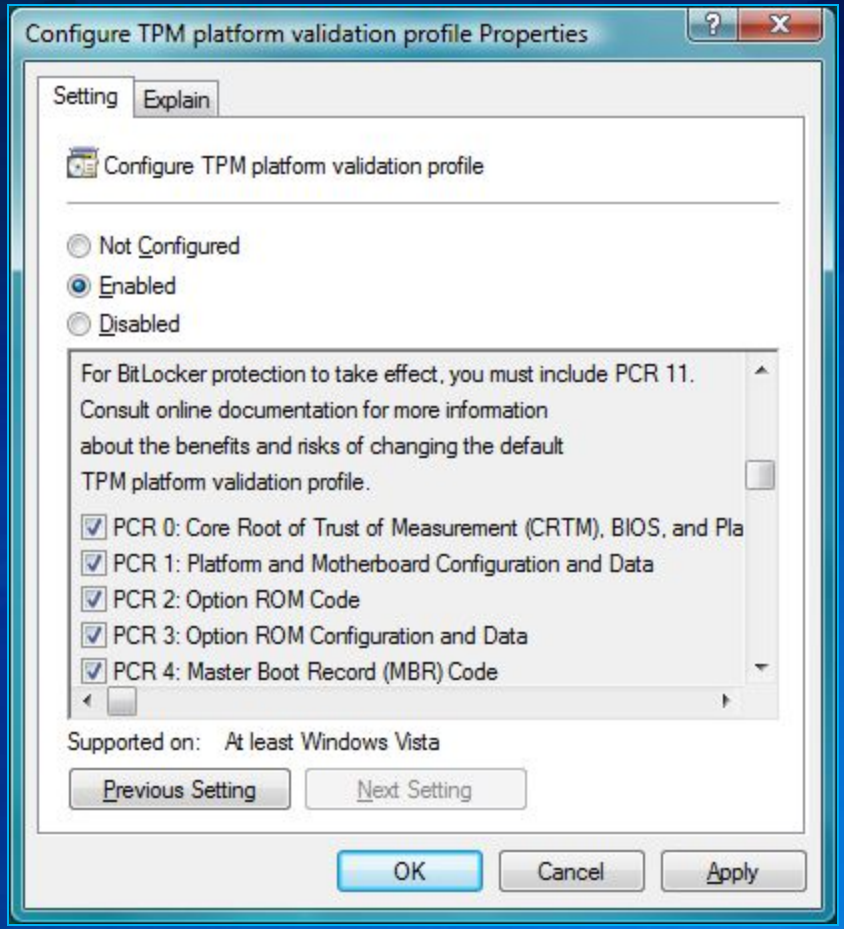
- Оранжевые – сервисы TPM
- Голубые – сервисы Microsoft
- Желтые и зеленые – сервисы сторонних производителей

BitLocker™ и TPM

- Шифрование диска BitLocker™
  - Шифрует полностью том
  - Использует Trusted Platform Module (TPM) v1.2 для проверки pre-OS компонентов
  - Настраиваемые методы защиты и аутентификации
- Защита до запуска ОС
  - USB ключи, PIN, TPM, аутентификация
- Единый драйвер TPM от Microsoft
  - Улучшеная стабильность и безопасость
- TPM Base Services (TBS)
  - Позволяет включать в цепочку приложение от сторонних поставщиков
- Active Directory Backup
  - Автоматизированное резервное копирование ключей в AD
  - Поддержка групповых политик
- Скриптовые интерфейсы
  - Управление TPM
  - Управление BitLocker™
  - Инструменты коммандной строки

Варианты применения BitLocker

Policy setting	Description	Windows Vista default
Turn on BitLocker backup to Active Directory Domain Services	Enables the backup of BitLocker recovery information in Active Directory. This recovery information includes the recovery password and some unique identifier data.	Not configured
Control Panel Setup: Configure recovery folder	Configures whether the BitLocker setup wizard asks the user to save the recovery key to a folder. Specifies the default path that displays when the BitLocker Setup Wizard prompts the user to type the location of a folder in which to save the recovery key.	Not configured
Control Panel Setup: Configure recovery options	Configures whether the BitLocker Setup Wizard asks the user to create a recovery password. The recovery password is a randomly generated 48-digit sequence.	Not configured
Control Panel Setup: Enable advanced startup options	Configures whether the BitLocker Setup Wizard asks the user to create a PIN on the computer. The PIN is a 4–20 digit sequence that the user types each time the computer starts. You cannot use policy to set the number of digits.	Not configured
Configure encryption method	Configures the encryption algorithm and key size that BitLocker uses. This policy setting applies to a fully decrypted disk. If the disk is already encrypted or if encryption is in progress, changing the encryption method has no effect.	Not configured
Configure TPM platform validation profile	Configures how the TPM secures the disk volume's encryption key. This policy setting does not apply if the computer does not have a compatible TPM, nor does changing this policy affect existing copies of the encryption key.	Not configured



Требования BitLocker

- Аппаратное обеспечение Trusted Platform Module
  - TPM не ниже версии 1.2
  - Логотип Vista certified
- Несовместимое с TPM оборудование
  - BIOS должен поддерживать загрузку с USB

Содержание

- Краткий обзор технологий защиты
- BitLocker
- Active Directory Rights Management Services

Rights Management Services

- RMS позволяет организациям создавать и применять политики использования информации, которой они владеют
  - Для любого приложения
  - В любом формате
- Политика использования «живет» вместе с информацией
  - Куда и каким бы способом ни перемещалась защищенная информация

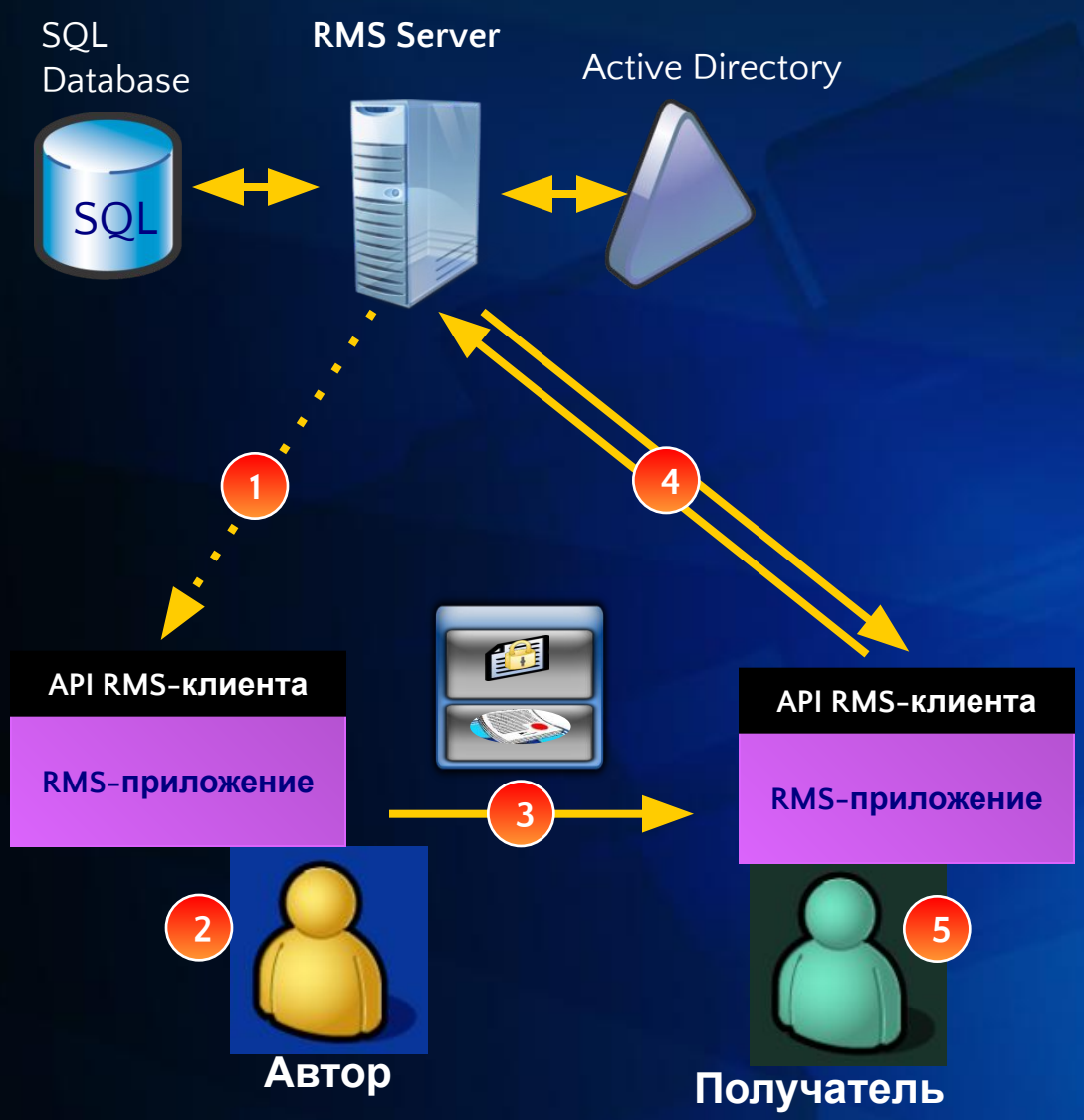
Rights Management Services

- Защита информации
  - Данные защищены во время хранения, передачи и обработки
  - Защита внутри и снаружи организации
- Применение политик
  - Постоянный контроль над тем, кто имеет доступ к документу, что он может с ним делать и как долго
- Контроль на уровне орга-низации
  - Централизованное управление политиками
  - Протоколирование информационных потоков
- Расширяемая платформа
  - Доступный программный интерфейс
  - Поддержка в приложениях Microsoft и третьих фирм

Rights Management Services

- Не поможет ограничить права на воспроизведение MP3
- Не обеспечит гарантированно невзламываемую систему безопасности
- Не защитит от аналоговых атак

Принцип действия RMS



1. При первом использовании RMS автор получает необходимые ключи и, возможно, политики, определенные отделом ИТ
2. Автор определяет/применяет политику к данным; приложение с помощью RMS-клиента шифрует данные и создает политику; приложение сохраняет политику вместе с зашифрованными данными
3. Автор распространяет файл
4. Получатель открывает файл; приложение вызывает RMS-клиента для авторизации пользователя и получения лицензии на использование
5. Приложение расшифровывает файл с помощью RMS-клиента и реализует указанные в лицензии права; RMS-клиент обеспечивает безопасность работы с данными

Microsoft Платформа 2008

Новые возможности

- Развертывание
  - Не требуется активация в MS Activation Service
  - Устанавливаются все требуемые службы
- Управление и администрирование
  - MMC-консоль для администрирования
  - Реализация всех функций скриптами
  - Генерация отчетов
  - Административные роли
- Взаимодействие с внешними организациями
  - Интеграция RMS со службами ADFS
- Распространение шаблонов

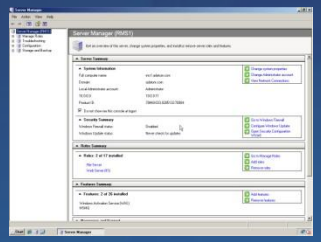
Внедрение

Развертывание инфраструктуры RMS

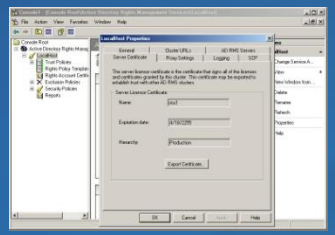
- Упрощенная установка настройка
  - Клиент RMS v2 встроен в Windows Server 2008 и Windows Vista
  - RMS – одна из серверных ролей
    - Автоматическая установка зависимых компонент (SQL Embedded, WPF, IIS, MSMQ, и др…)
  - Новый мастер решает все задачи, связанные с настройкой RMS
  - Автоматическое обнаружение и регистрация RMS-клиентов
- Функциональная независимость
  - Все необходимые сертификаты выдаются автономно, не требуется взаимодействие с сервисами Microsoft
  - Нет ограничения на срок действия корневого сертификата
- Обратная совместимость
  - Обновление сохраняет все защищенные до этого документы
  - Возможно взаимодействие с RMS-серверами предыдущей версии

Интерфейс

Установка RMS



Срок действия сертификата



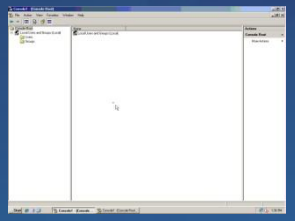
Среда работы

Управление RMS

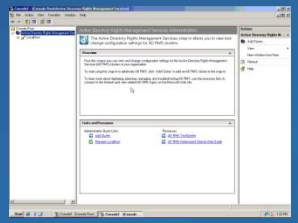
- Улучшения для администратора
  - Отказ от Web-интерфейса версии 1.0
  - Использование оснастки в консоли MMC……
    - Знакомая административная модель
    - Единый подход ко всем серверным ролям
  - Выделение задач (обязательных, рекомендованных, дополнительных)
    - Выполнение «задач под рукой»
  - Ролевое администрирование
    - Администраторы предприятия, шаблонов, аудиторы
- Администрирование с помощью скриптов
  - Задачи управления доступны через Scripting API

Интерфейс

Управление на основе задач



Роли администратора



Эффективность

Основные направления развития

- Усовершенствованные мониторинг и отчетность
- Общее повышение производительности

Модернизация модели «здоровья» RMS

- Управление на основе событий
- Обработка ошибок – более конкретные и подробные
- Метрики
  - Перехват специфичных для RMS событий

MOM 2005 Management Pack

- После Beta 2

Анализ журнала

- Интегрированный инструмент генерации отчетов

Microsoft Платформа 2008

Внешнее взаимодействие

Довери-тельные отношения	• Обе организации должны развернуть RMS • Одно- или двусторонний обмен сертификатами для включения доверительных отношений
Extranet-записи	• Добавление записей в AD для внешних пользователей • Прохождение SSL-трафика ко внутр. RMS-серверам • Использование сертификатов для аутентификации • Использование VPN для усиления защиты
Hosted Services	• Использование Windows Live ID • Решения партнеров
Federated RMS	• Двустороннее взаимодействие, развертывание RMS только в одной организации • Обе организации настраивают ADFS

Типовой сценарий

Adatum

Крупная производственная компания

Федеративные отношения с Contoso

Обмен конфиденциальными данными между сотрудниками Adatum **и** Contoso

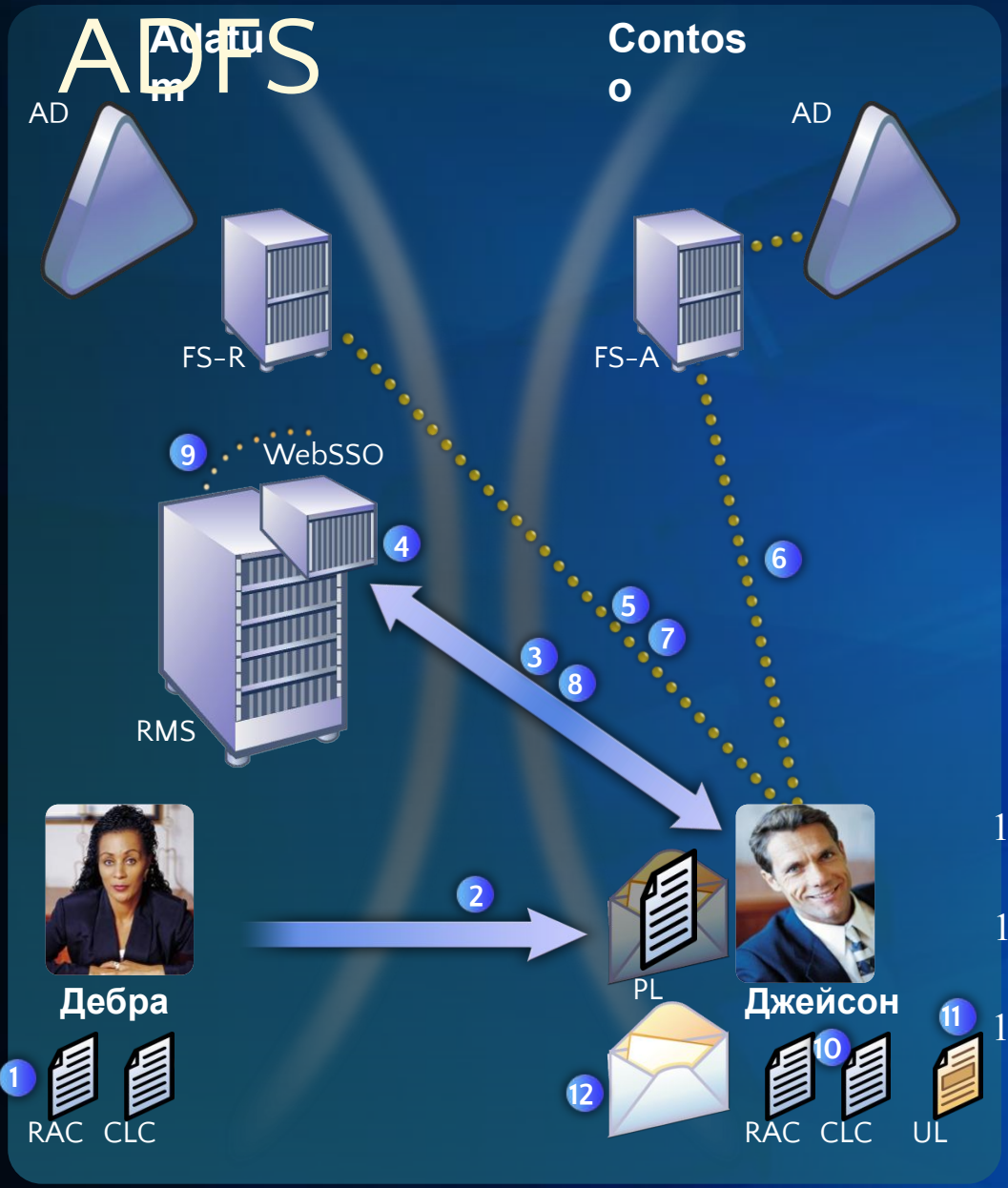
Debra

Contoso

PR-услуги для Adatum

Jason

Взаимодействие на основе ADFS



1. Дебра применяет политику к письму
2. Дебра посылает защищенное письмо Джейсону в Contoso
3. Компьютер Джейсона обращается к RMS-серверу
4. Агент ADFS перехватывает запрос
5. RMS-клиент перенаправляется FS-R для аутентификации
6. RMS-клиент перенаправляется FS-A для аутентификации
7. Сформированная заявка (claim) возвращается к FS-R
8. RMS-клиент запрашивает UL
9. WebSSO-агент перенаправляет запрос RMS-серверу
10. RMS-сервер возвращает сертификат RAC Джейсону
11. RMS-сервер формирует и передает Джейсону UL
12. Джейсон получает доступ к содержимому письма

Платформа Microsoft 2008

Требования

- Домен ресурсов
  - Полностью подготовленная инфраструктура RMS
  - Federation Server (Windows Server 2003 R2 или 2008)
  - SSL на вирт. каталогах RMS и на Federation Server
- Домен учетных записей
  - Federation Server (Windows Server 2003 R2 или 2008)
  - SSL на Federation Server

Распространение шаблонов

- Основная проблема: настройка на клиентах вручную
- Новый метод на базе SOAP для получения шаблонов
- RMS-клиент в Vista SP1 поддерживает автоматическое обновление шаблонов с сервера
  - Новый API в клиенте RMS для получения шаблонов
  - WMI-задание по расписанию вызывает API для получения шаблонов

Развитие RMS

Office 2007 Q4 CY06	• SharePoint (MOSS) 2007 • InfoPath 2007 • Усовершенствование пользовательского интерфейса
Windows Vista & XPS Q4 CY06	• RMS “встроен” в Windows Vista • Переход на Windows Presentation Foundation
Windows Mobile 6 Q2 CY07	• Поддержка смартфонов и КПК • Pocket Outlook и Pocket Office
Exchange 2007 SP1 Q4 CY07	• Технология Pre-licensing для RMS-сообщений • Первый шаг в интеграции с Exchange
Решения партнеров	•Система архивации с поддержкой RMS • Защита документации CAD

Microsoft®
Платформа
2008

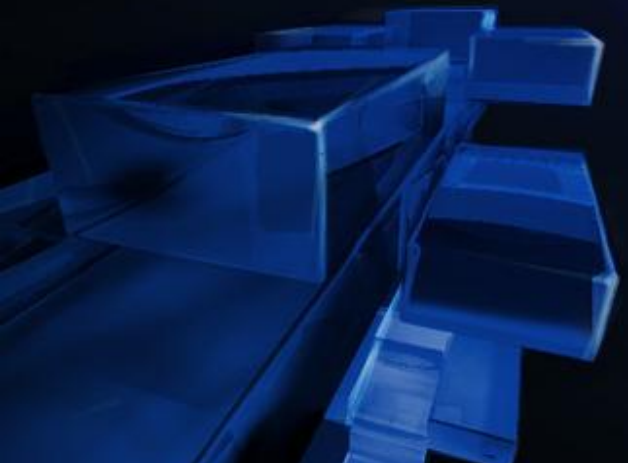
Службы Active Directory Rights Management Services

ДЕМОНСТРАЦИЯ

Microsoft Платформа 2008

ВОПРОСЫ?

Александр Шаповал
Microsoft
ashapo@microsoft.com
http://blogs.technet.com/ashapo



Microsoft®

Your potential. Our passion.™

Microsoft Платформа 2008