

Внешний доступ к службам RMS

Александр Шаповал
Microsoft

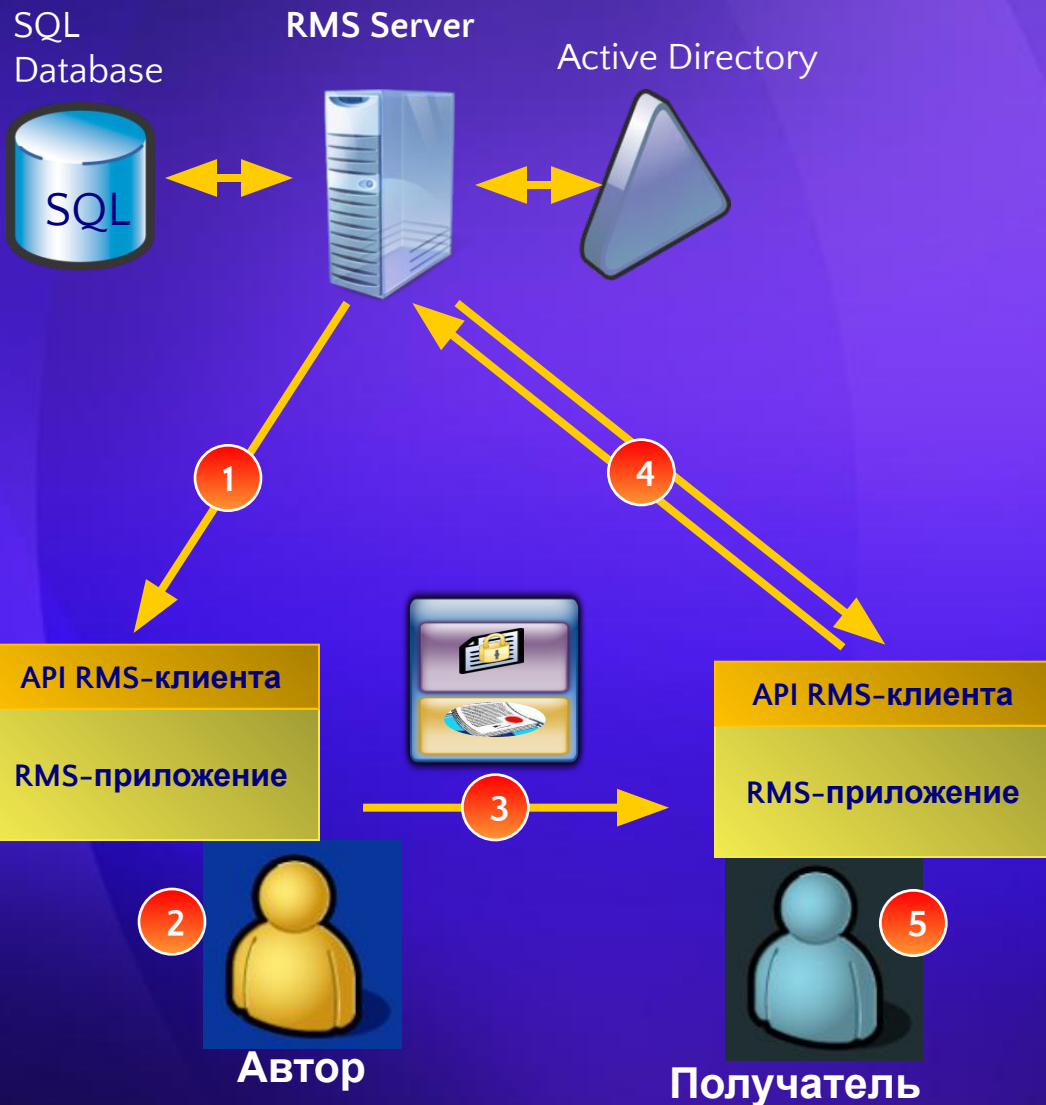
Содержание

- Принцип действия
- Бизнес-требования
- Технические требования
- Публикация RMS с помощью ISA Server 2006
- Сценарии внешнего доступа
 - Базовая архитектура
 - Бизнес – бизнес
 - Федеративные службы
 - Бизнес – пользователь (Windows Live ID)

Содержание

- Принцип действия
- Бизнес-требования
- Технические требования
- Публикация RMS с помощью ISA Server 2006
- Сценарии внешнего доступа
 - Базовая архитектура
 - Бизнес – бизнес
 - Федеративные службы
 - Бизнес – пользователь (Windows Live ID)

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

Содержание

- Принцип действия
- **Бизнес-требования**
- Технические требования
- Публикация RMS с помощью ISA Server 2006
- Сценарии внешнего доступа
 - Базовая архитектура
 - Бизнес – бизнес
 - Федеративные службы
 - Бизнес – пользователь (Windows Live ID)

Внешний доступ к RMS

Для чего?

- Наиболее часто **забываемый** аспект при развертывании RMS
- Сотрудникам необходим доступ к защищенной информации при использовании
 - Outlook RPC/HTTPS
 - Outlook Web Access
 - Документов Microsoft Office
 - Windows Mobile 6.0
- Если внешний доступ к RMS не настроен, пользователи не смогут работать с защищенными документами (кроме случаев использования VPN)

Внешний доступ к RMS

Бизнес-требования

- Информация может храниться и использоваться различными способами
- Обмен информацией внутри и между организациями – общее требование
- Критическая информация должна быть доступна из любого места
- Мобильность и гибкий доступ к данным – критическое требование для мобильных пользователей

Содержание

- Принцип действия
- Бизнес-требования
- **Технические требования**
- Публикация RMS с помощью ISA Server 2006
- Сценарии внешнего доступа
 - Базовая архитектура
 - Бизнес – бизнес
 - Федеративные службы
 - Бизнес – пользователь (Windows Live ID)

Внешний доступ к RMS

Технические требования

- Мобильные пользователи
 - Если письмо или документ не открывался во внутренней сети, требуется аутентификация и UL
 - Если документ скопирован с одного компьютера на другой, требуется аутентификация и UL
 - Если задан срок действия лицензии, или документ требует постоянного подключения, пользователю необходим доступ к серверу RMS, даже если этот пользователь уже имеет UL
 - Exchange 2007 SP1 Pre-licensing Fetching минимизирует эти требования, однако некоторые вложения и другие документы требуют связь с RMS-сервером

Внешний доступ к RMS

Технические требования

- Внешний доступ к кластеру RMS
 - RMS-конвейер (URL-ссылки) должен быть доступен из Internet
 - В качестве альтернативы можно настроить VPN, но это ограничивает использование таких продуктов и технологий, как:
 - Outlook RPC/HTTP
 - OWA
 - Windows Mobile 6
 - MOSS 2007

Внешний доступ к RMS

Технические требования

- Внешний доступ
 - Не включен по умолчанию
 - Должен определяться на стадии планирования развертывания служб RMS
 - Должен рассматриваться, даже если изначально не требуется
 - Любой защищенный документ содержит URL сервера лицензирования (конвейера)

Внешний доступ к RMS

Технические требования

- Внешний доступ
 - Если внешний доступ включается уже после применения RMS к определенным документам, необходимо:
 - Снять защиту с документов
 - Очистить папку DRM в профиле пользователя
 - Настроить внешний доступ на сервере RMS
 - Снова защитить документы
 - Распространить новые версии файлов

Вывод: продумывайте внешний доступ на этапе планирования

Внешний доступ к RMS

RMS-конвейеры для внешнего доступа

- **Сертификаты- /_wmcs/certification/***
 - Используется для получения пользователем Rights Accounts Certificate (RAC)
 - Доступ необходим при первом использовании служб RMS
 - Доступ запрещен за пределами интрасети для защиты структуры RMS
 - Может влиять на некоторые приложения
 - OWA

Внешний доступ к RMS

RMS-конвейеры для внешнего доступа

- **Лицензии** - `/_wmcs/Licensing/*`
 - Используется для получения Use Licenses (UL) для каждого защищенного документа и
 - Client Licensing Certificates (CLC) для защиты в режиме Offline
 - Должен быть виден снаружи для реализации внешнего доступа
 - В зависимости от сценария может требоваться соответствующая аутентификация

Содержание

- Принцип действия
- Бизнес-требования
- Технические требования
- Публикация RMS с помощью ISA Server 2006
- Сценарии внешнего доступа
 - Базовая архитектура
 - Бизнес – бизнес
 - Федеративные службы
 - Бизнес – пользователь (Windows Live ID)

RMS и ISA Server 2006

- ISA Server 2006 сокращает поверхность атак благодаря следующим возможностям:
 - Пакетная фильтрация
 - Аутентификация
 - Ограничение путей
 - SSL-мост
 - Фильтрация уровня приложений

RMS and ISA 2006

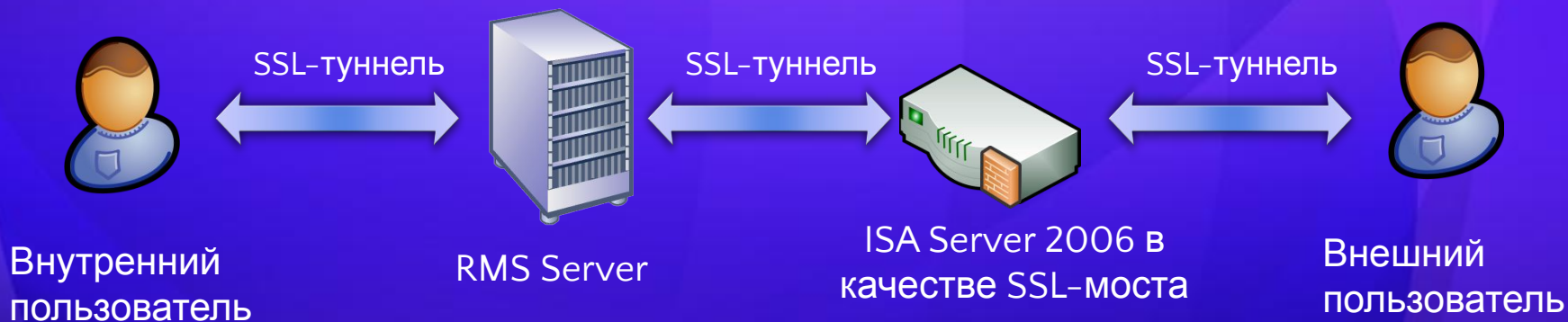
Ограничение путей

- Преимущества
 - Доступ к строго определенным виртуальным каталогам и asmx-файлам сервера RMS
 - Windows RMS V1.0
 - `/_wmcs/certification/*`
 - `/_wmcs/licensing/*`
 - Active Directory RMS V2.0 с опцией ADFS Integration
 - `/_wmcs/certificationexternal/*`
 - `/_wmcs/licensingexternal/*`

RMS и ISA 2006

SSL-мост

- Для конвейеров сертификатов и лицензий
- Рекомендуемый подход, поскольку IIS может иметь только один сертификат на веб-сайт



RMS и ISA 2006

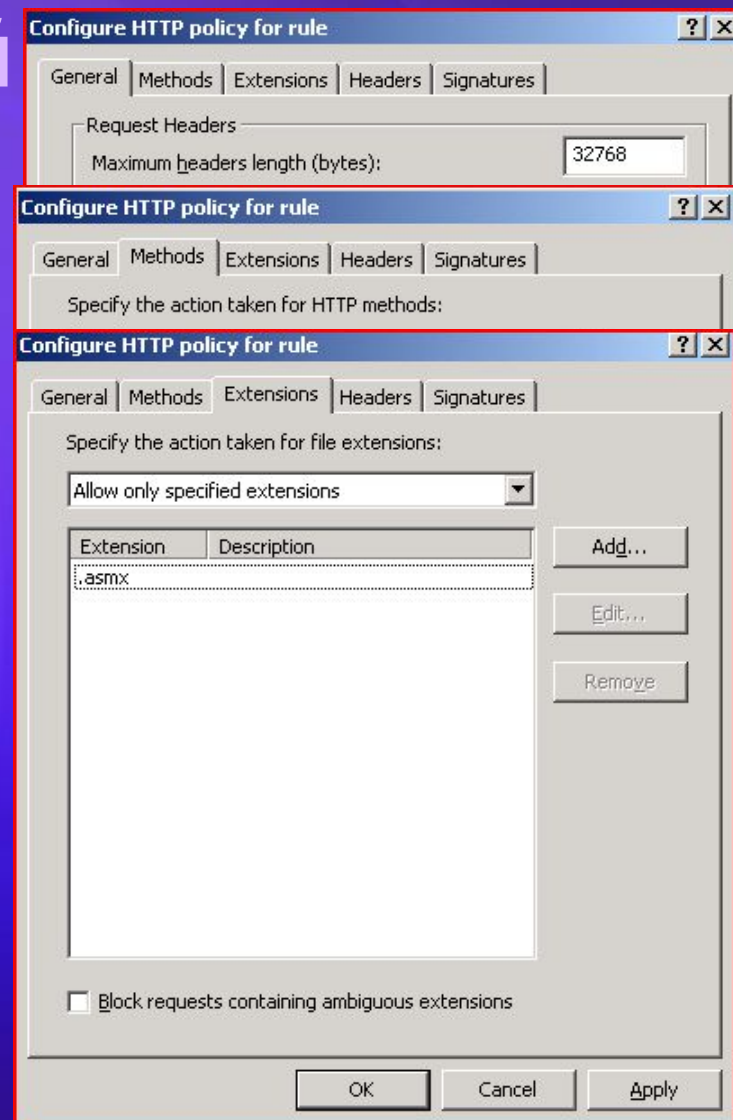
SSL-МОСТ

- **Возможности**
 - Проверка SSL-трафика на вредоносный код
 - Различные внешние и внутренние имена для конвейеров
 - Внешний конвейер – Сертификат на ISA Server 2006
 - Пример:
 - <https://rms.contoso.com/>
 - Внутренний конвейер – Сертификат на кластере RMS
 - Пример:
 - <https://rms.contoso.local/>
 - **Замечание:** на IIS 6 допустимо применение Subject Alternative names, однако не все провайдеры поддерживают эту функцию

RMS и ISA 2006

Фильтрация приложений

- General
 - Max. URL Length – 256 bytes
 - Max. Query Length – 256 bytes
 - Verify Normalization – включено
 - Block High Bit Characters – включено
 - Block Responses with Executables – включено
- Methods
 - Разрешить только POST, SOAP, GET
- Extensions
 - Разрешить только файлы .asmx



RMS и ISA 2006

RMS в зоне периметра

- **Входящий трафик**
 - HTTPS TCP/443 и HTTP/80 (не рекомендуется для внешнего доступа)
- **Исходящий трафик от RMS к DC**
 - Kerberos (88/tcp и 88/udp)
 - DCE RPC (135/tcp, 135/udp, динамические порты)
 - NetBIOS/SMB (137-139, 445/tcp и udp)
 - LDAP, ICMP, NTP
- **Исходящий трафик от RMS к SQL**
 - 1433/TCP

Содержание

- Принцип действия
- Бизнес-требования
- Технические требования
- Публикация RMS с помощью ISA Server 2006
- **Сценарии внешнего доступа**
 - Базовая архитектура
 - Бизнес – бизнес
 - Федеративные службы
 - Бизнес – пользователь (Windows Live ID)

Внешний доступ к RMS

Сценарии

- Базовая архитектура
 - Базовый сценарий
 - Несколько лесов, доверенные домены
- Бизнес – бизнес
 - Доверенные домены
 - Федеративные службы
- Бизнес – пользователь
 - Windows Live ID

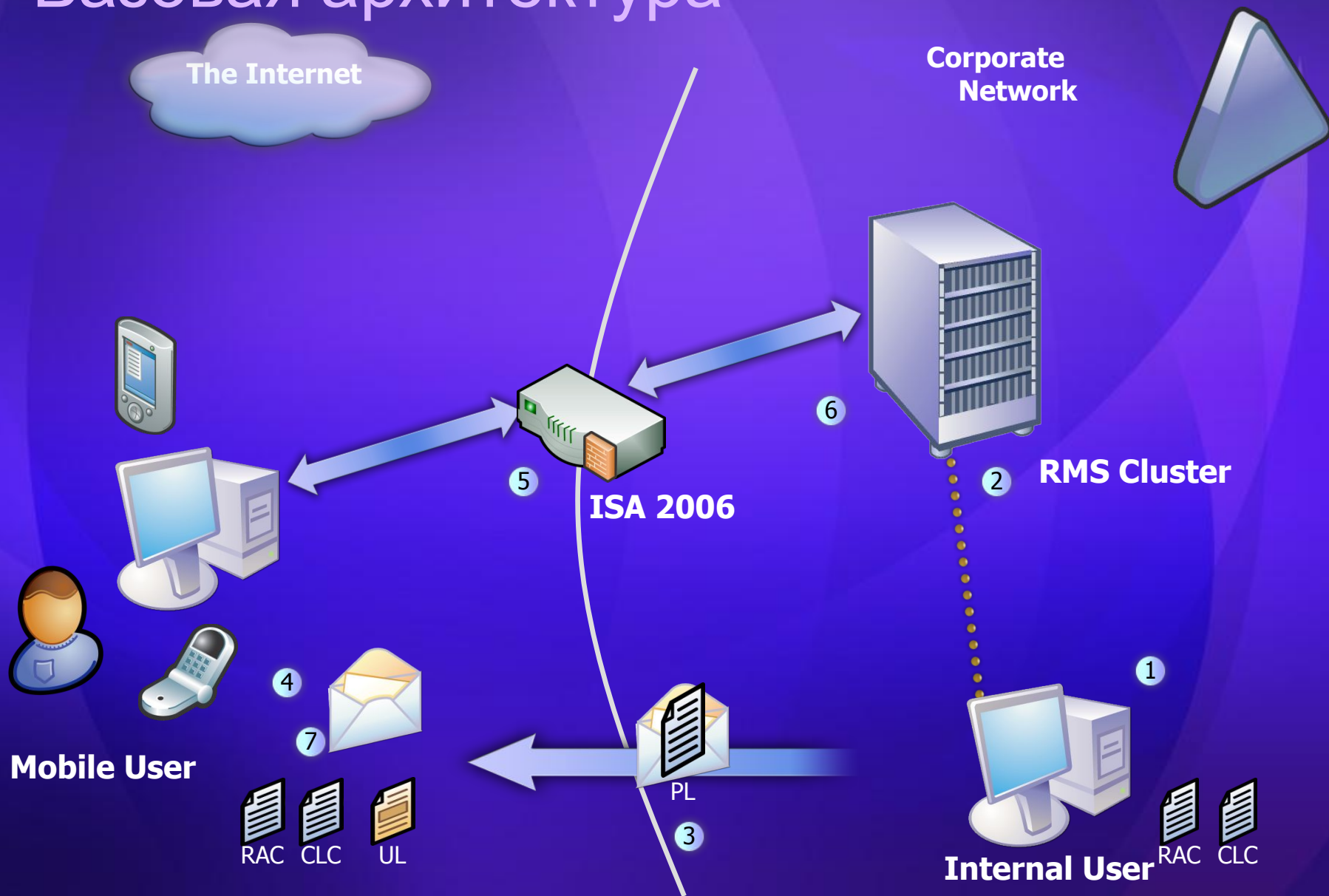
Внешний доступ к RMS

Базовая архитектура

- Наиболее простой сценарий
 - С защищенными документами работают только корпоративные пользователи
- Требования бизнеса
 - Доступ к документам с ноутбуков, мобильных устройств, возможно, с домашних компьютеров

Внешний доступ к RMS

Базовая архитектура



Внешний доступ к RMS

Базовая архитектура

- **Публикация**

#	Pipeline	Virtual Directory	Files	Purpose/Role
1	Certification	/_wmcs/Certification/	Certification.asmx	RAC acquisition
2	Licensing	/_wmcs/Licensing/	License.asmx Publish.asmx	License and CLC acquisition

- **Аутентификация**

- Требуется

- **Набор типовых правил на ISA Server**

- Одно правило публикации RMS
- Одно правило для SSL-сертификата

Внешний доступ к RMS

Несколько лесов

- **Публикация**
 - Как в базовом сценарии
- **Аутентификация**
 - Требуется
- **Набор типовых правил на ISA Server**
 - Зависит от доверительных отношений
 - Конвейер сертификатов необходим, если нужна удаленная активация клиентов (1 на лес)
 - Конвейеры лицензий можно консолидировать:
<http://www.microsoft.com/technet/itshowcase/content/deprmswp.msp>

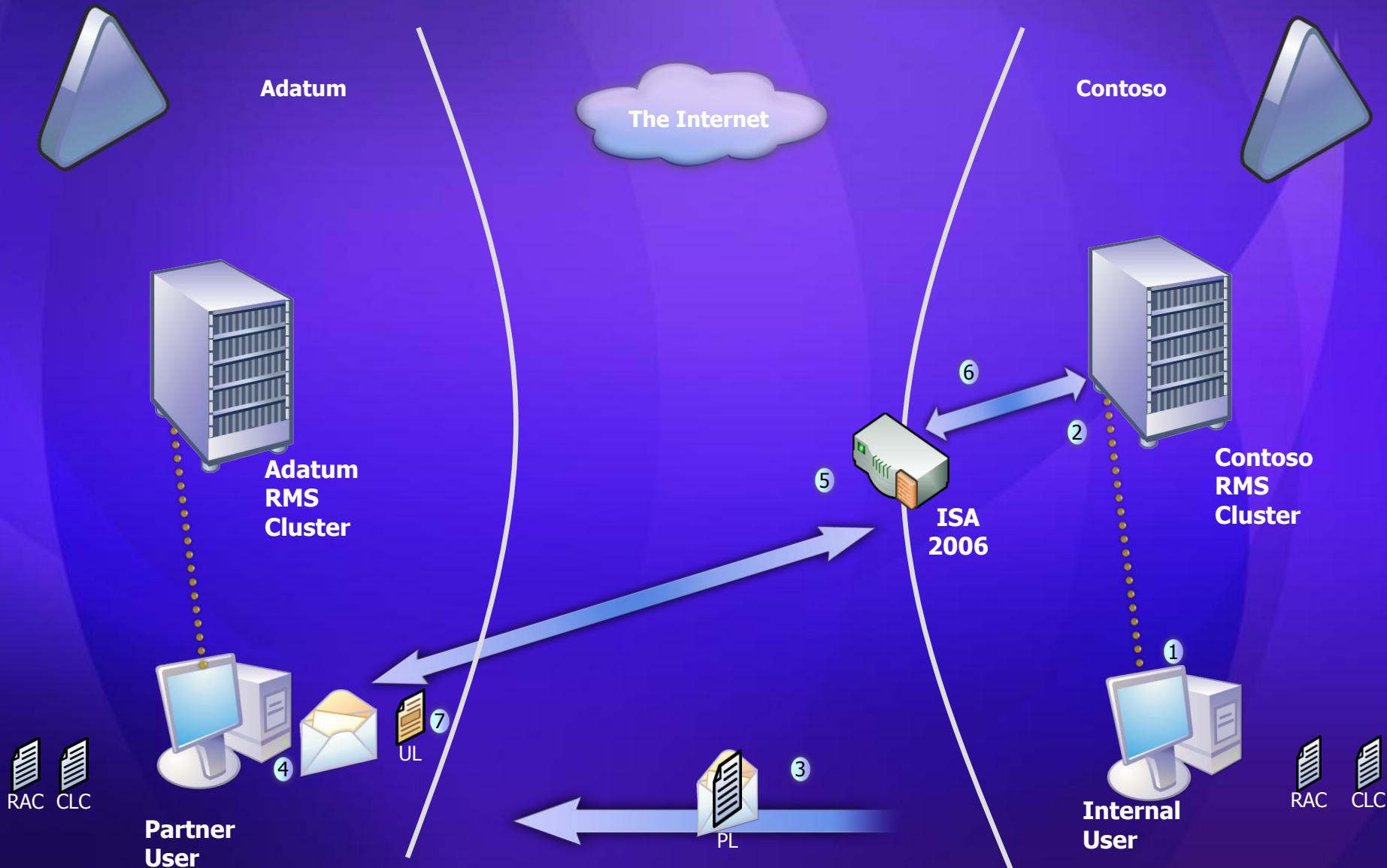
Внешний доступ к RMS

Бизнес – бизнес

- Для взаимодействия с внешними организациями
 - Обычно применяется Trusted User Domains (TUD)
 - В Windows 2008 добавляется интеграция с ADFS, существенно расширяющая использование RMS

Внешний доступ к RMS

Бизнес – бизнес, TUD



Внешний доступ к RMS

Бизнес – бизнес, TUD

- **Публикация**

#	Pipeline	Virtual Directory	Files	Purpose/Role
1	Certification	/_wmcs/Certification/	Certification.asmx	RAC acquisition
2	Licensing	/_wmcs/Licensing/	License.asmx Publish.asmx	License.asmx configured <u>anonymous</u>

- **Аутентификация**

- Требуется для получения сертификата
- Не требуется для получения лицензии

- **Набор типовых правил на ISA Server**

- Два правила публикации RMS
- Одно правило для SSL-сертификата

Типовой сценарий

Adatum

Крупная производственная компания

Федеративные отношения с Contoso

Обмен конфиденциальными
данными между сотрудниками
Adatum и Contoso



Дебра

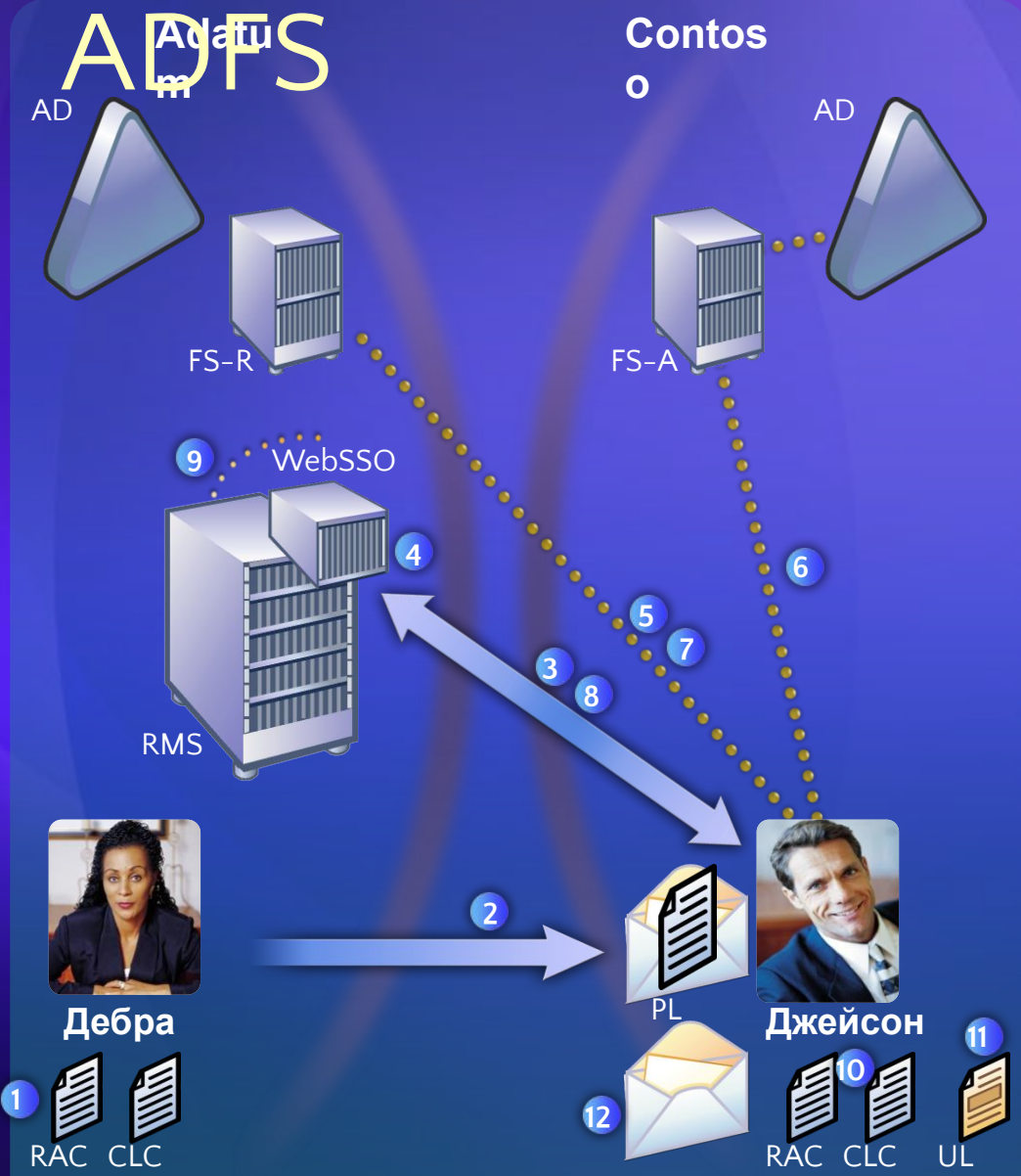
Contoso

PR-услуги для
Adatum



Джейсон

Взаимодействие на основе



1. Добра применяет политику к письму
2. Добра 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

Внешний доступ к RMS

Бизнес – бизнес, ADFS

- Публикация

#	Pipeline	Virtual Directory	Files	Purpose/Role
1	Certification	/_wmcs/Certification/	Certification.asmx	RAC acquisition
2	Licensing	/_wmcs/Licensing/	License.asmx Publish.asmx	License and CLC acquisition
3	Certification and Licensing	/_wmcs/Certificationexternal/ /_wmcs/Licensingexternal/	*	RAC, Licensing and CLC request from ADFS Clients
4	ADFS	/adfs/ls/	*	ADFS-R Service

Внешний доступ к RMS

Бизнес – бизнес, ADFS

- **Аутентификация**
 - Требуется для получения сертификата (внутренними пользователями)
 - Не требуется для конвейеров RMS/ADFS
 - Не требуется для федеративных отношений
- **Набор типовых правил на ISA Server**
 - 1 правило для публикации RMS, 1 правило для публикации ADFS
 - Два правила для SSL-сертификата

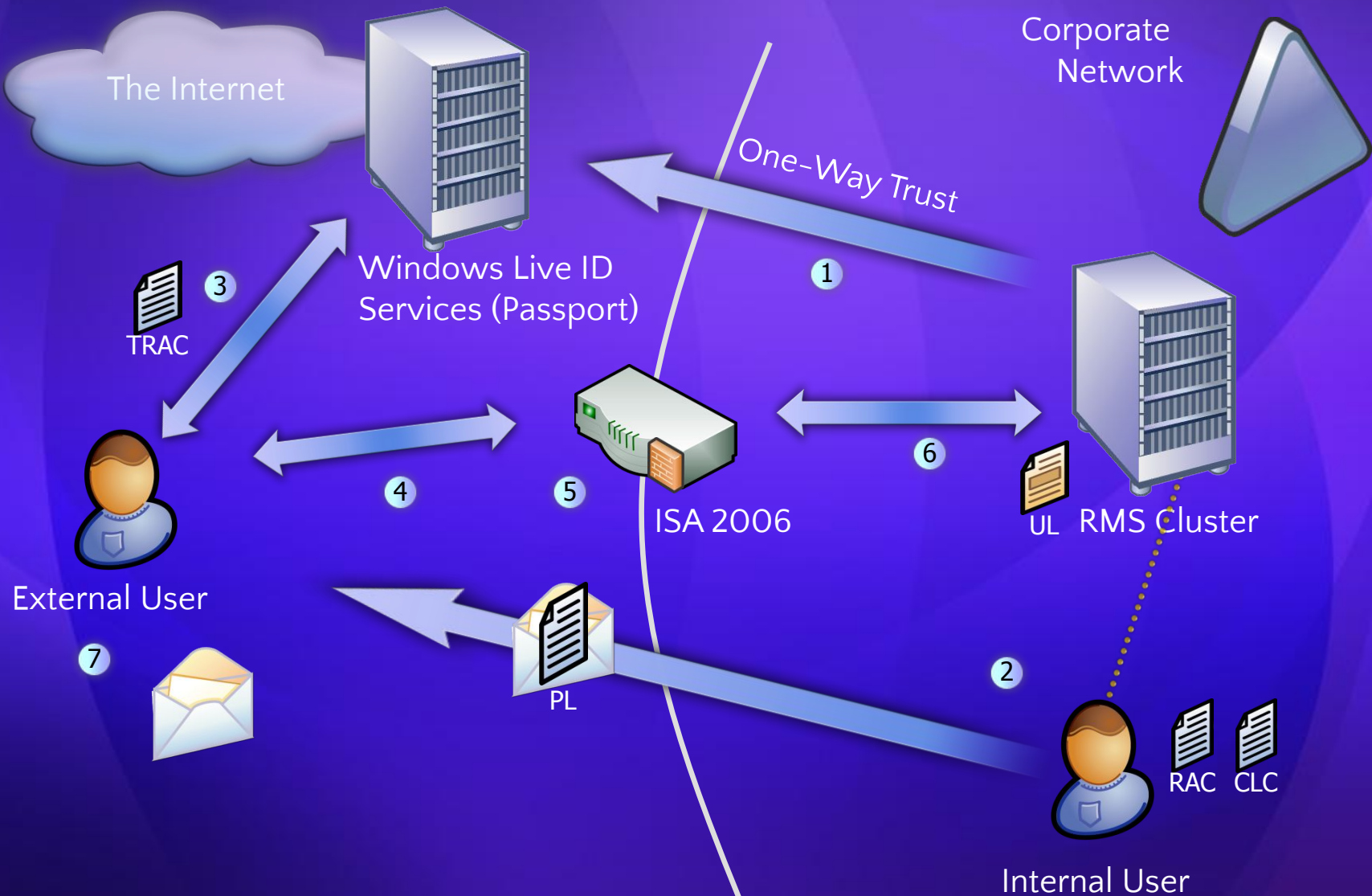
Внешний доступ к RMS

Бизнес – пользователь

- Для взаимодействия с внешними субъектами, не имеющими RMS
 - Обычно используется Windows Live ID
- Для реализации устанавливаются доверительные отношения между RMS-сервером и службой Windows Live ID
 - Одноразовая операция, RMS-серверу требуется доступ в Internet на этапе конфигурации
- Одностороннее взаимодействие – между пользователями Windows Live ID
- Публикуется RMS-конвейер лицензий

Внешний доступ к RMS

Windows Live ID



Вопросы

- <http://blogs.technet.com/ashapo>
- Особенности служб сертификации в Windows Server 2008
 - Веб-трансляция, 20 ноября
 - <http://www.microsoft.com/rus/technet>

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.