

Решения Microsoft в области управления идентификацией и доступом

... в контексте модели оптимизации инфраструктуры

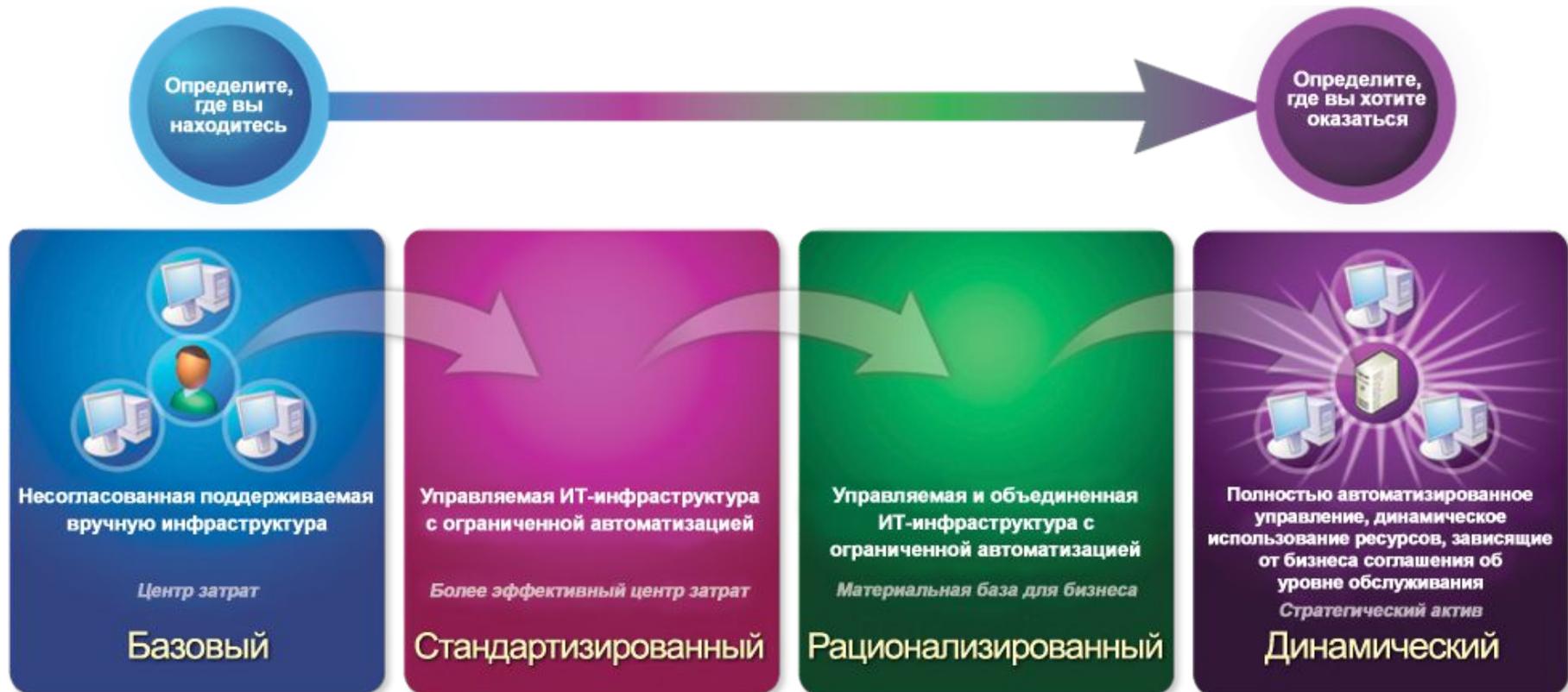
Дмитрий Алтухов, Optimicon
dmitry@altukhov.com



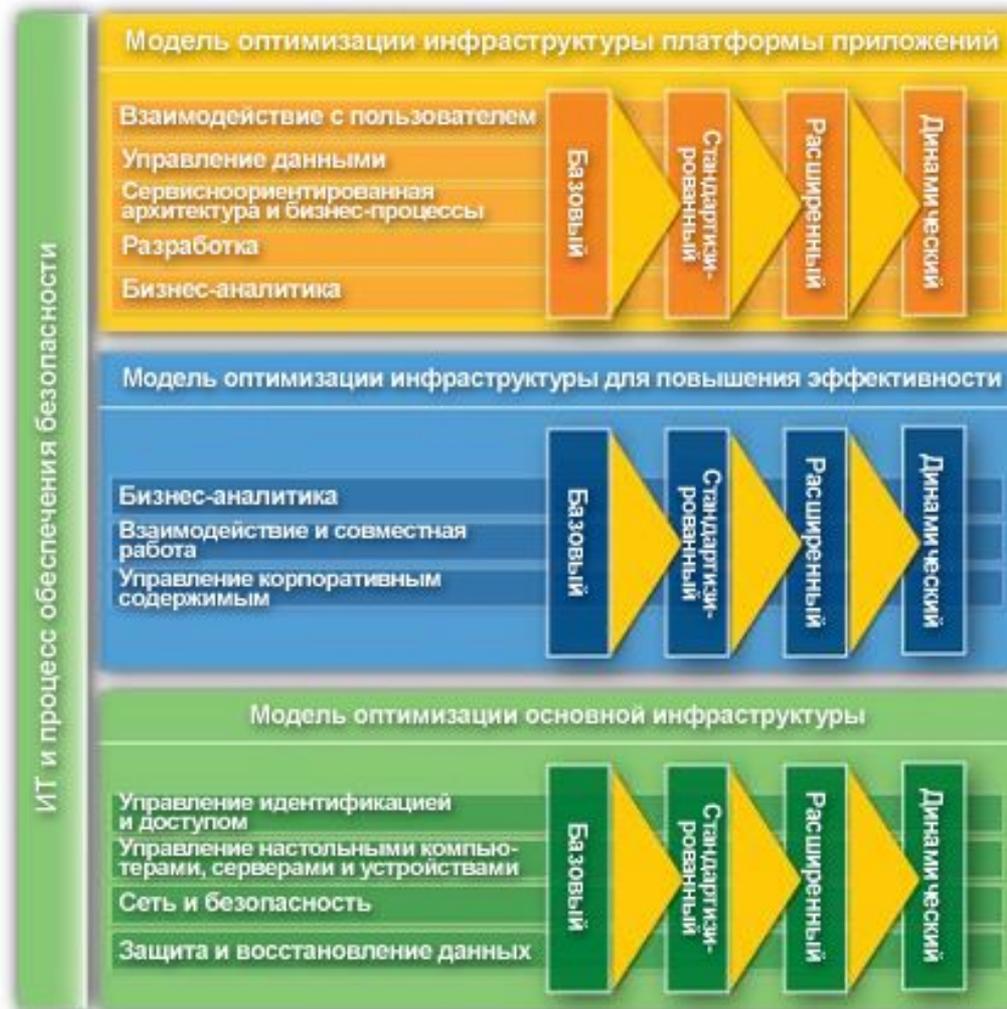
О компании «Оптимикон»

- Компания создана в 2007 году в составе группы СРМ
- Сертифицированный партнер Microsoft
 - компетенция Security Solutions
 - специализация Identity and Access Management
- Основная методология - модель оптимизации инфраструктуры Microsoft
- Команда, работающая с инфраструктурными решениями Microsoft с 2000 года
- Все ключевые продукты и технологии –
 - Windows Server/Active Directory,
 - Exchange Server,
 - System Center Configuration Manager & Operations Manager (ранее – SMS и MOM)
 - Security (ISA, Forefront, PKI)
 - Виртуализация
- Проекты по развертыванию и миграции AD 2000 – 2003 – 2008, Exchange 2000 – 2003 – 2007 и т.п.
- Аутсорсинг с возможностью поддержки 24/7/365 на базе СРМ

Уровни зрелости ИТ инфраструктуры



Три модели оптимизации



Оптимизация основной инфраструктуры

- **Управление идентификацией и доступом**
 - Active Directory, групповые политики, управление жизненным циклом учетных записей
- **Управление настольными компьютерами, устройствами и серверами**
 - Стандартизация настольных операционных систем
 - Управление правами пользователей
 - Консолидация и виртуализация
 - Автоматизация обновлений
 - Мониторинг серверов
- **Сеть и безопасность**
 - Межсетевые экраны
 - Антивирус, антиспам - централизация
- **Защита и восстановление данных**
 - Автоматизация архивирования и восстановления

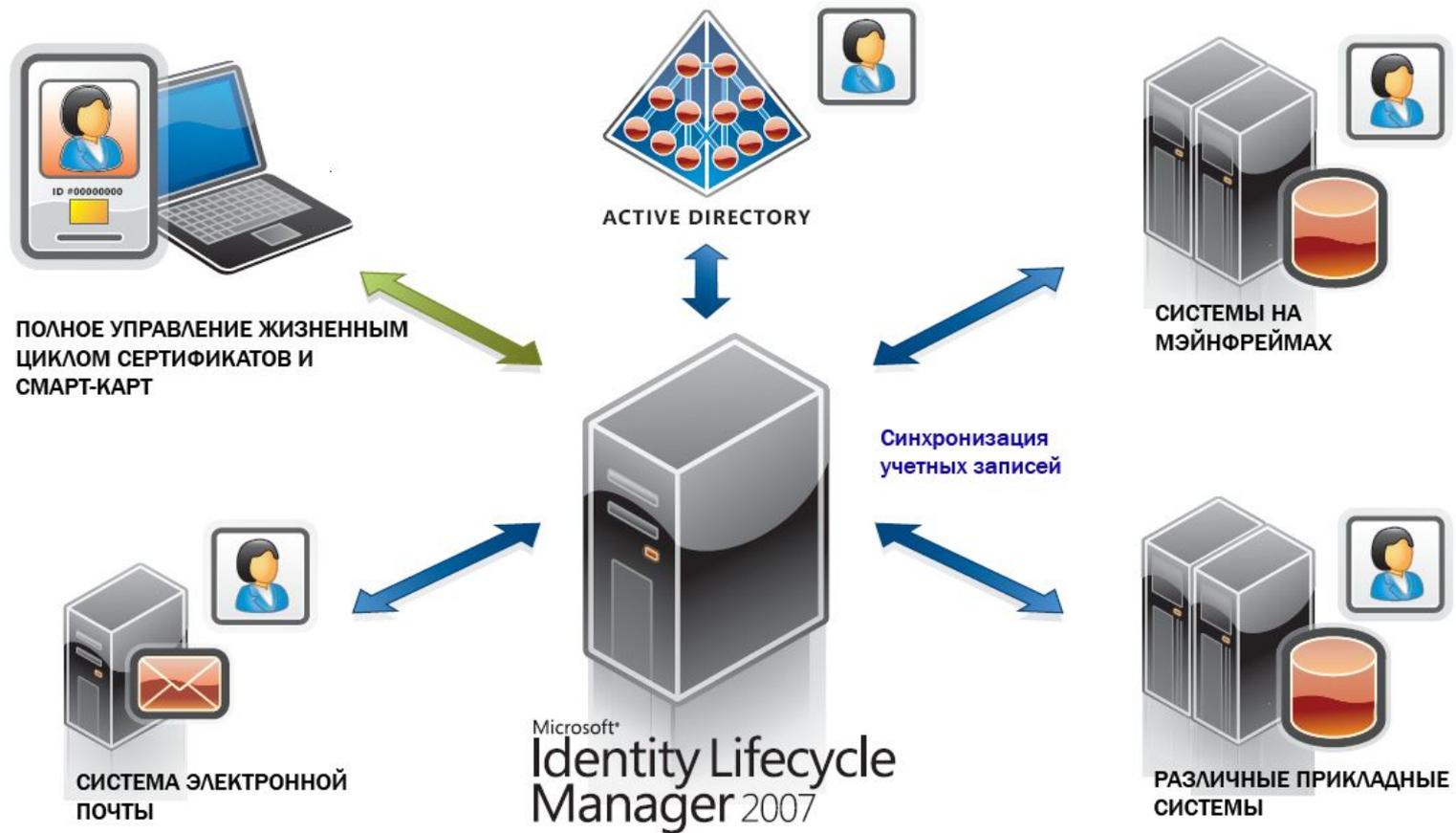


Концепция управления идентификацией и доступом

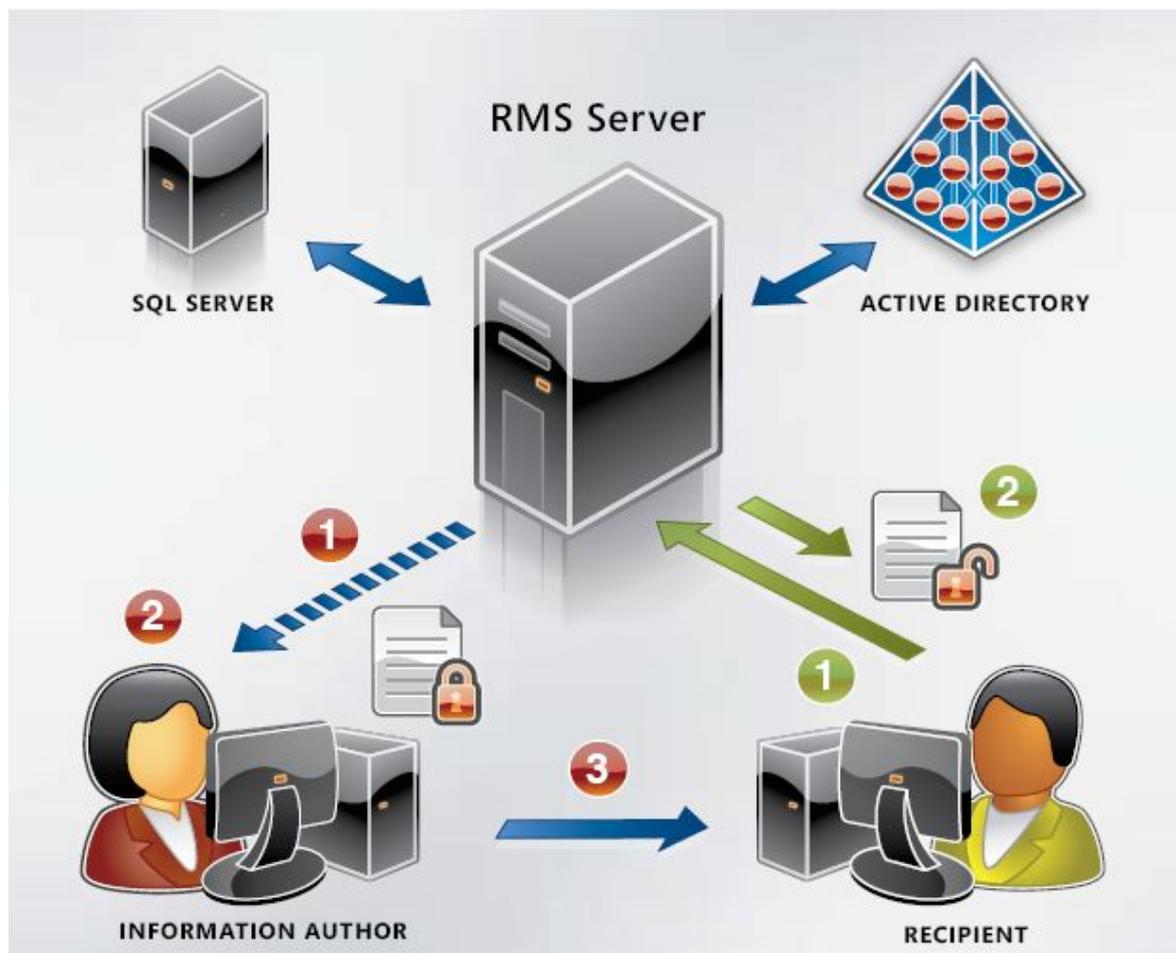
- **Управление жизненным циклом**
 - Автоматизация управление идентификацией и доступом
- **Защита информации**
 - Защита конфиденциальных данных, где бы они не находились
- **Федеративная идентификация**
 - Безопасная совместная работа разных организаций
- **Сильная и многофакторная аутентификация**
 - Безопасный доступ, основанный не только на именах и паролях
- **Службы каталогов**
 - Упрощенное управление пользователями и устройствами



Управление жизненным циклом



Защита информации



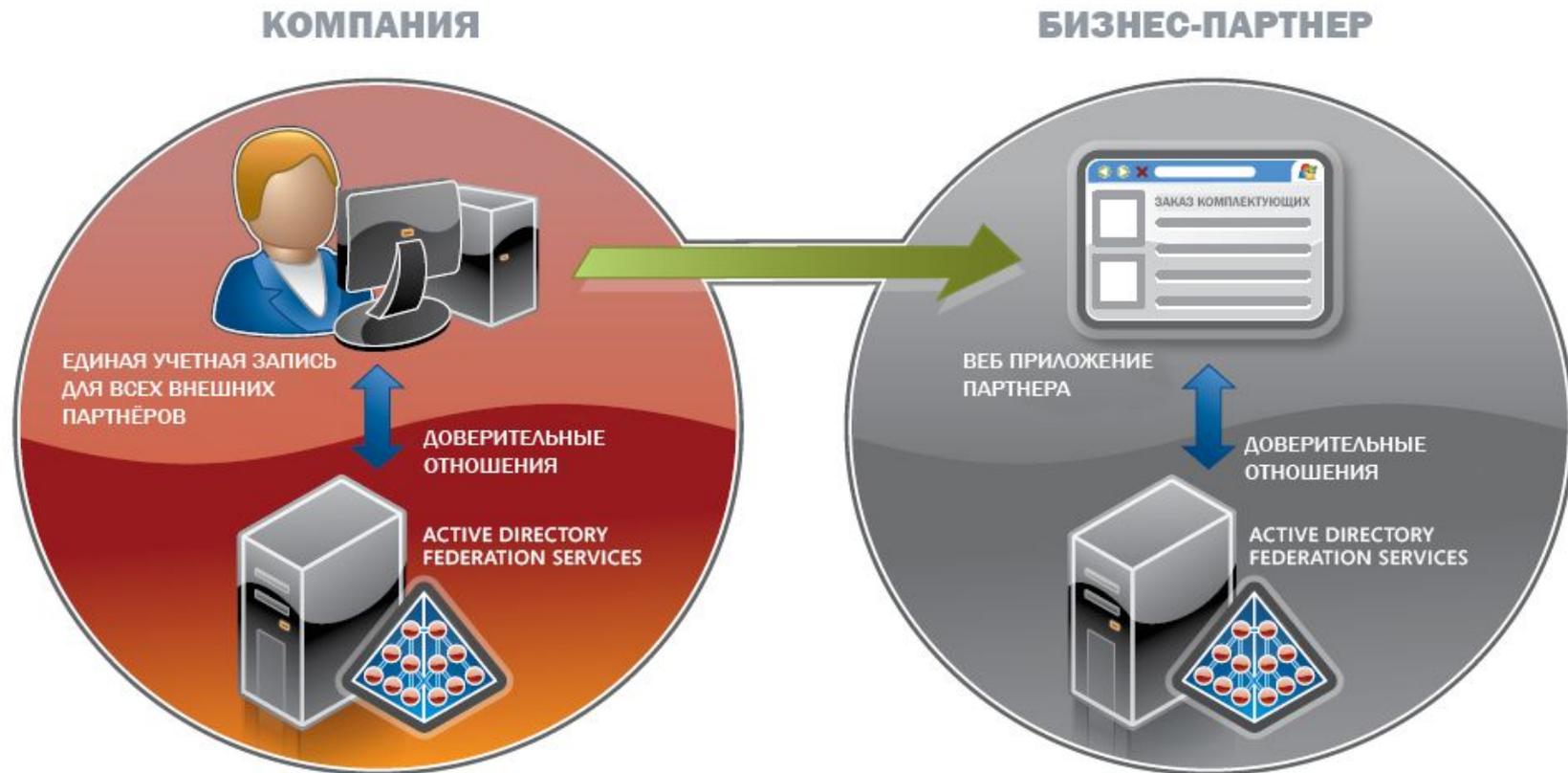
ДЕЙСТВИЯ АВТОРА

- 1** Автор автоматически получает сертификат лицензиара при первом использовании сервера управления правами доступа
- 2** Автор определяет набор прав использования, приложение создает «лицензию издателя» и шифрует файл
- 3** Автор распространяет файл

ДЕЙСТВИЯ ПОЛУЧАТЕЛЯ

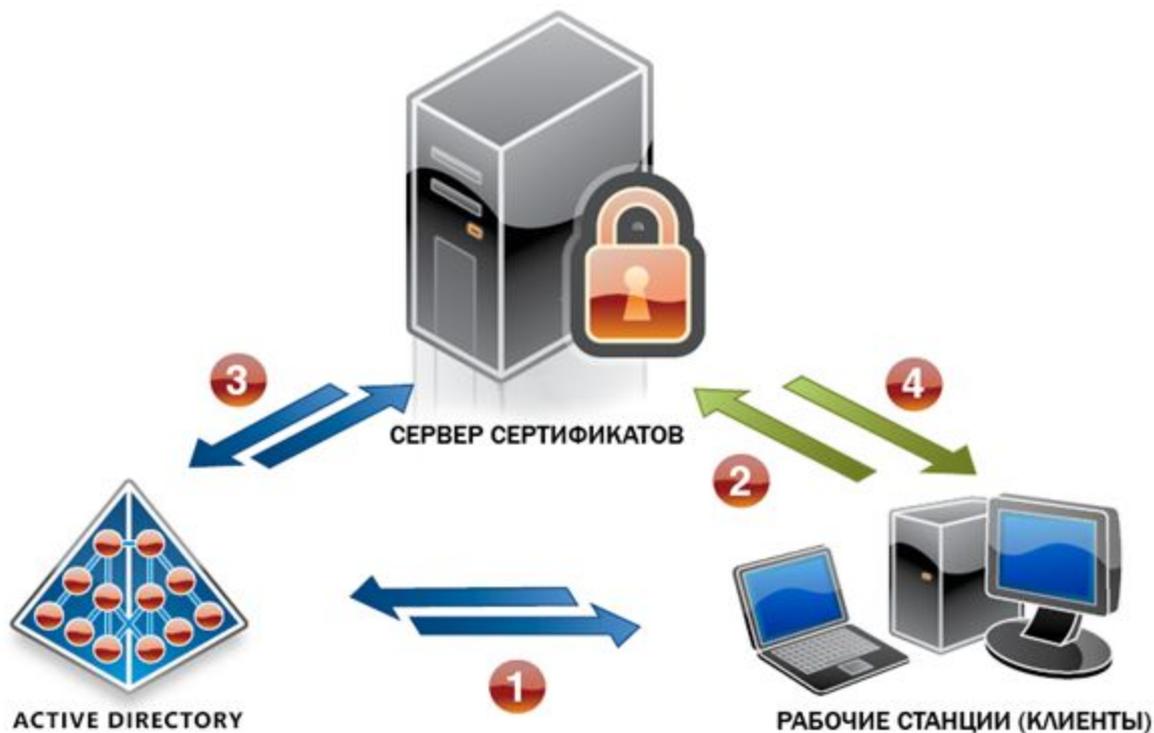
- 1** При попытке открытия файла получателем приложение обращается к серверу управления правами доступа, который проверяет права использования и выдает «лицензию читателя»
- 2** Приложение декодирует и открывает файл в соответствии с правами пользователя

Федеративная идентификация



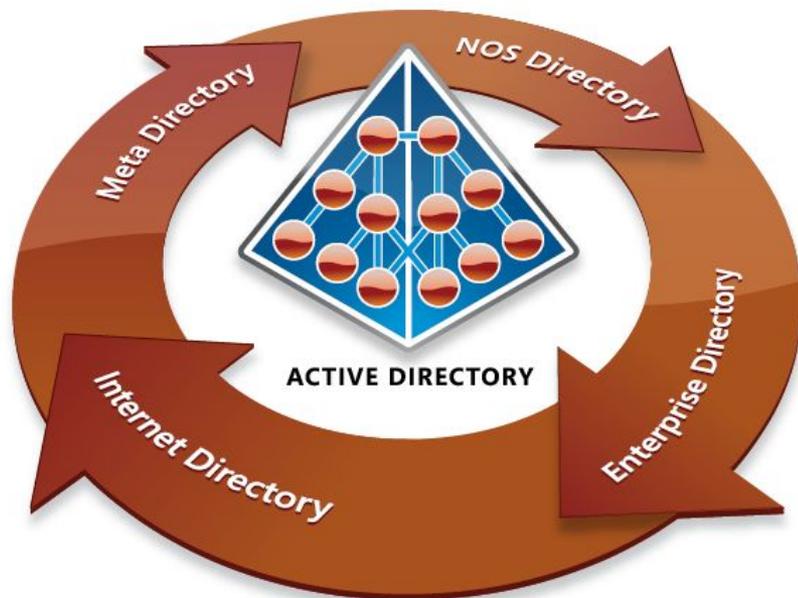
Сильная и многофакторная аутентификация

WINDOWS CERTIFICATE SERVICES

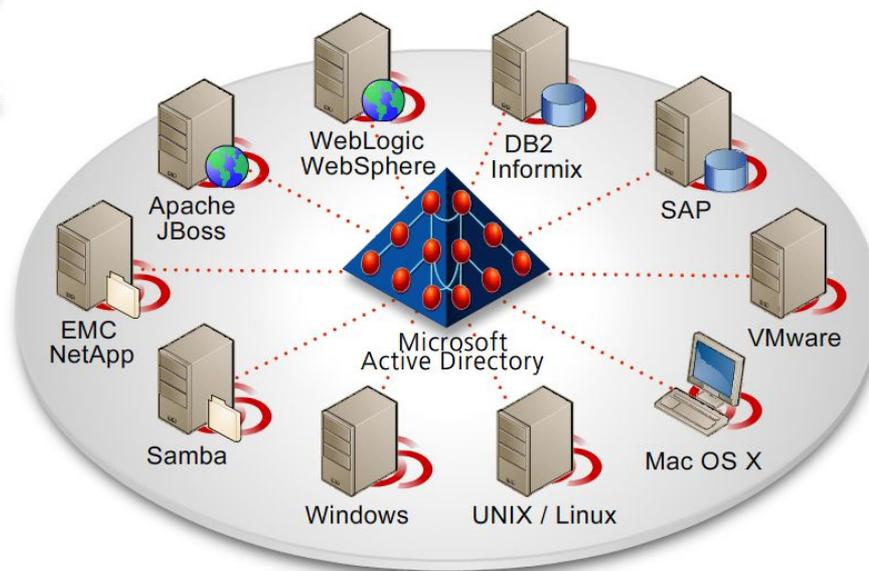


- 1** Клиент извлекает политику сертификатов из Active Directory
- 2** В соответствии с политикой клиент делает запрос к серверу сертификатов
- 3** Сервер сертификатов извлекает данные пользователя из Active Directory
- 4** Сервер сертификатов возвращает клиенту подписанный цифровой сертификат

Службы каталогов



- Active Directory Domain Services
- Active Directory Lightweight Directory Services (LDAP), ранее Active Directory Application Mode (ADAM)
- Интеграция с другими системами и службами каталогов



Спасибо за внимание



Дмитрий Алтухов
dmitry@altukhov.com
www.optimicon.com