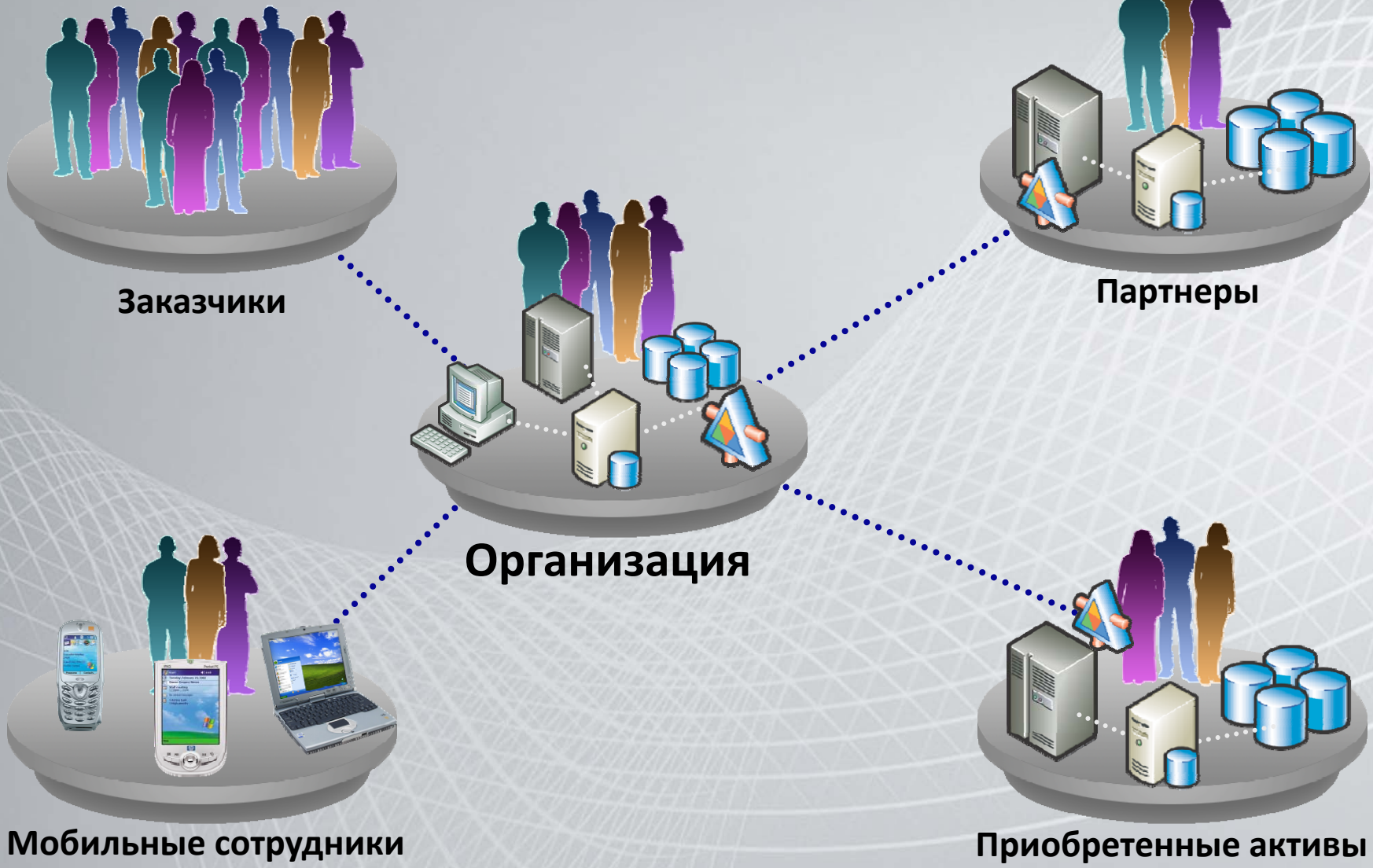
Построение систем защищенного взаимодействия

Алексей Голдбергс
i-alexg@microsoft.com
http://blogs.technet.com/securityrus
Microsoft Россия

Сценарии доступа

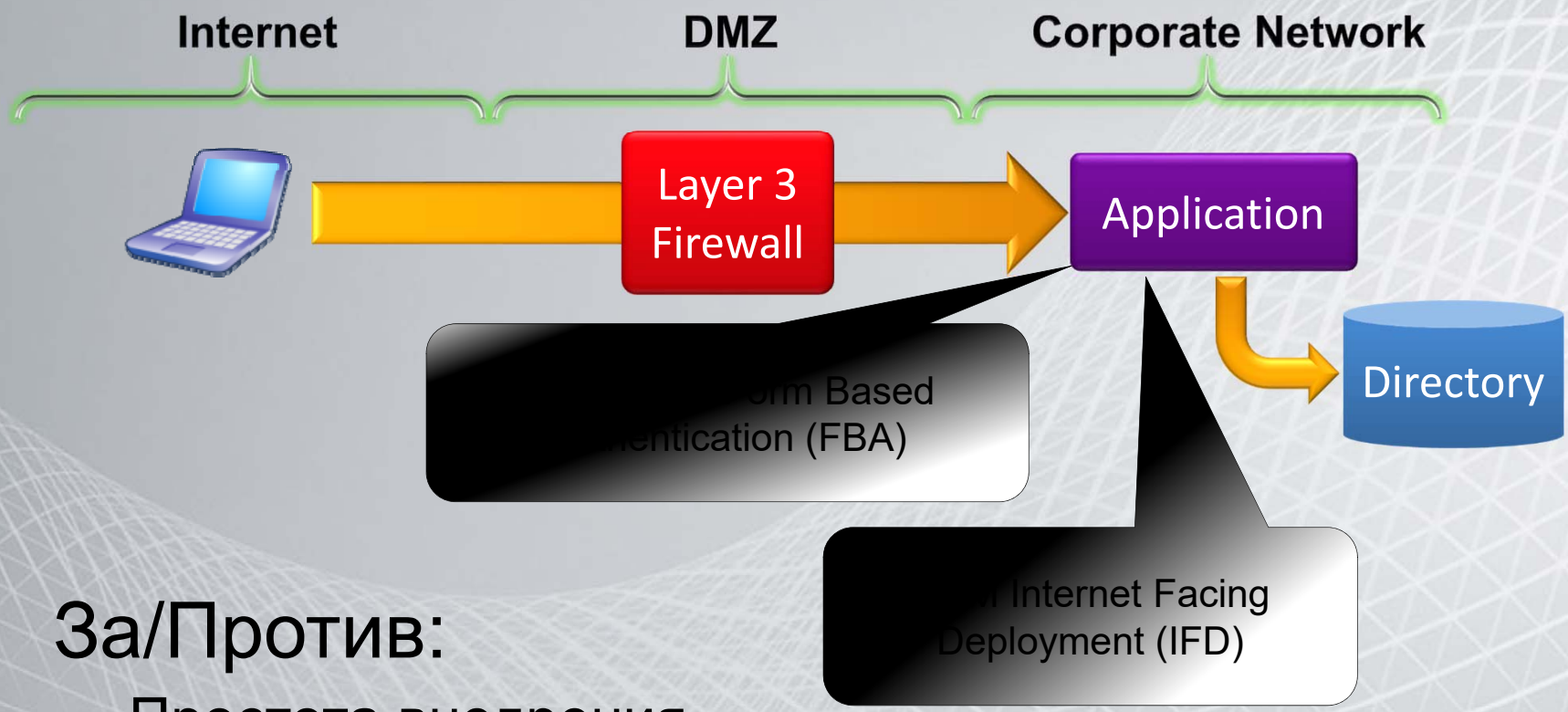


Задача

Предоставить доступ к бизнес-приложениям сотрудникам, партнерам и конечным заказчикам

Архитектура удаленного доступа

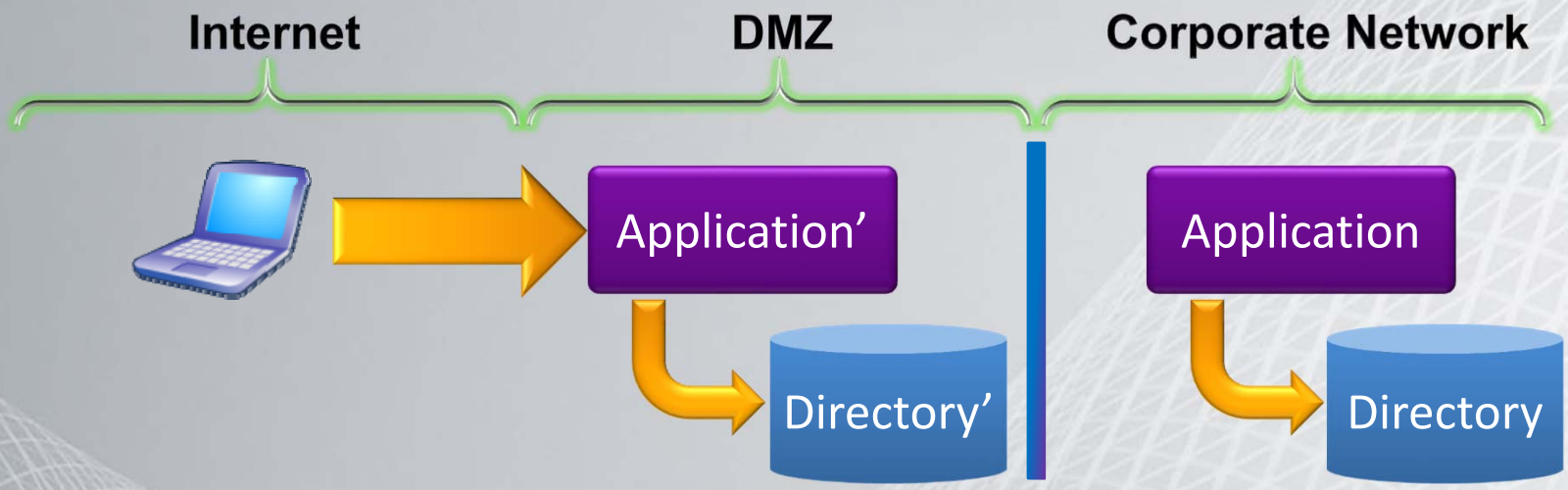
Открытый Intranet



- За/Против:
  - Простота внедрения
  - Ограниченные возможности защиты
  - Ограниченная поддержка SSO
  - Внутренние приложения уязвимы для Internet

Архитектура удаленного доступа

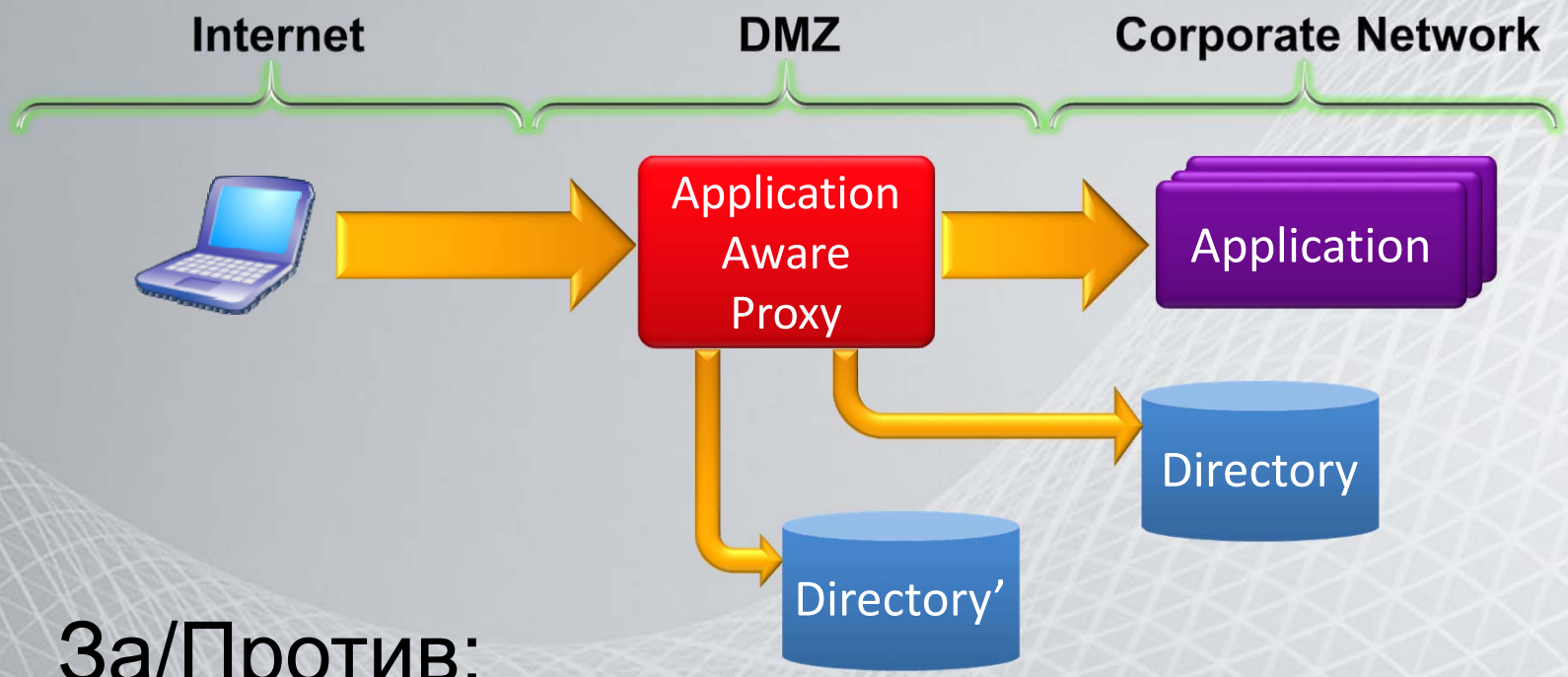
Изолированный Extranet



- За/Против:
  - Безопасность через изоляцию
  - Дублирование систем
  - Сотрудники не могут взаимодействовать с партнерами
  - Приложения в DMZ уязвимы для Internet

Архитектура удаленного доступа

Публикация



- За/Против:
  - Простота внедрения
  - Отсутствие дублирования
  - Изоляция прикладного уровня
  - Поддержка SSO и строгой аутентификации

Почему публикация безопасна?

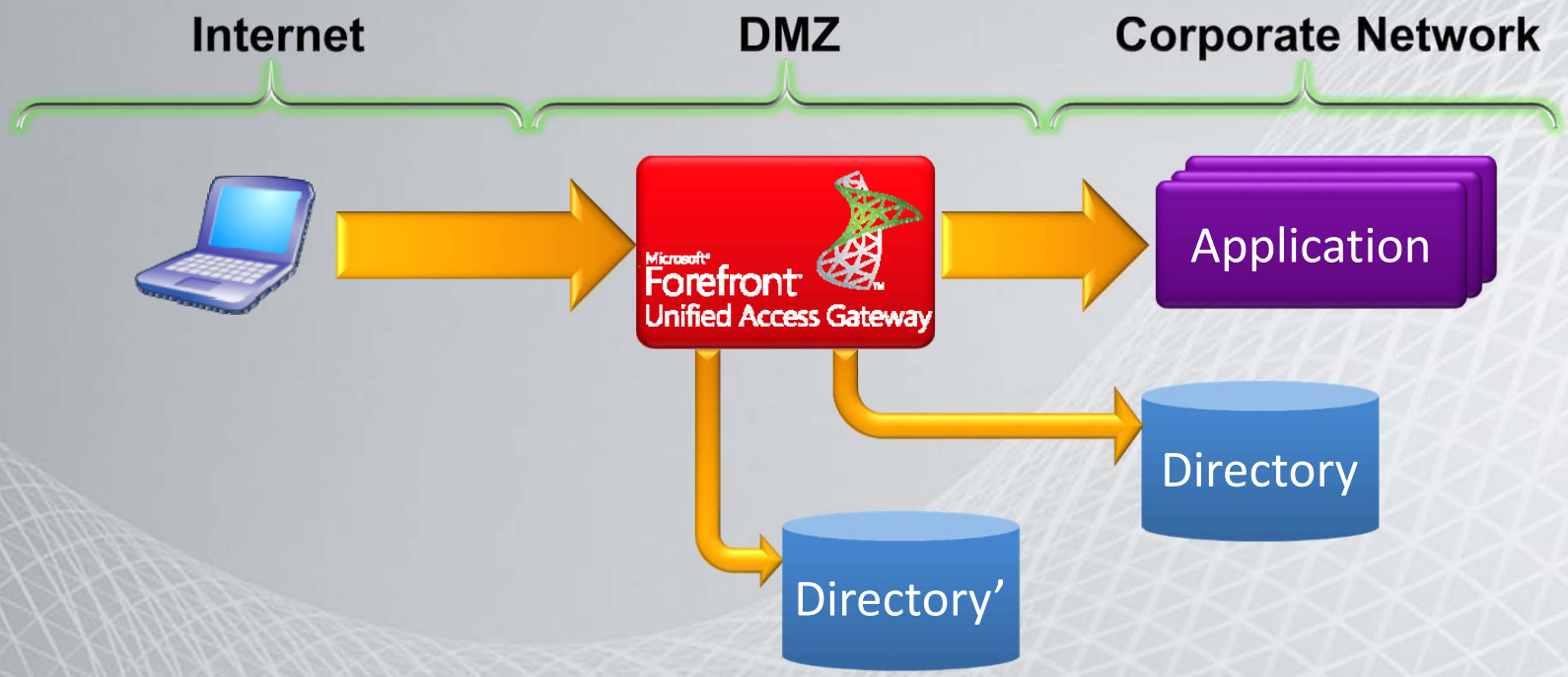
- Доступ только для аутентифицированных пользователей – Защита серверов приложений от DDoS
- Понимание прикладного уровня (например перенаправление только допустимых HTTP-запросовs) – Уменьшение поверхности атаки
- Тайм-ауты – Уменьшения риска hijacking сессии

Почему публикация лучше для конечных пользователей?

- Единая точка входа во все приложения – как правило в виде портала
- Single Sign-On (SSO) между различными приложениями и ресурсами корпоративной сети

Архитектура удаленного доступа

Публикация



Microsoft® Forefront™ Unified Access Gateway

UAG предоставляет безопасный удаленный доступ из любой точки мира к любым бизнес-приложениям, повышая эффективность работы пользователей, не снижая общего уровня безопасности

Свободный доступ

- Единая точка доступа к бизнес-приложениям (Exchange, SharePoint, Dynamics CRM, SAP, Lotus) и другим внутренним ресурсам
- Поддержка всех наиболее распространенных интернет-браузеров (IE, Mozilla, Safari) и операционных систем (Windows, Mac OS X, Linux)

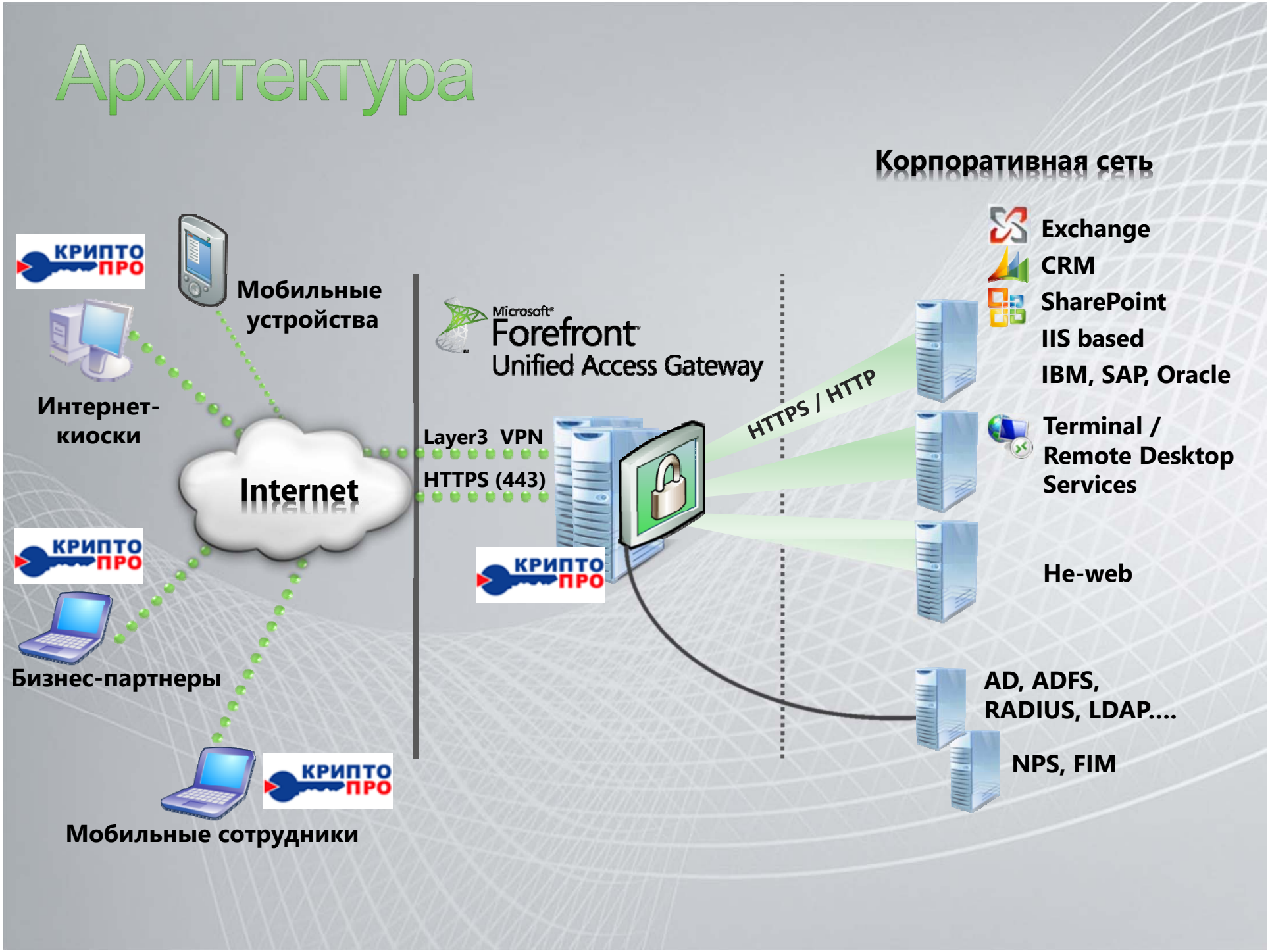
Повышенная безопасность

- Проверка конечных точек на соответствие требованиям политик безопасности
- Интеграция со службой Active Directory (включая Federation Services) и средствами многофакторной аутентификации
- Ограничение доступа к информации и снижение рисков утечки данных

Легкое управление

- Простота внедрения и эксплуатации посредством встроенных мастеров настройки
- Централизованное управление политиками доступа к приложениям
- Масштабируемость и отказоустойчивость

Архитектура



Федерация

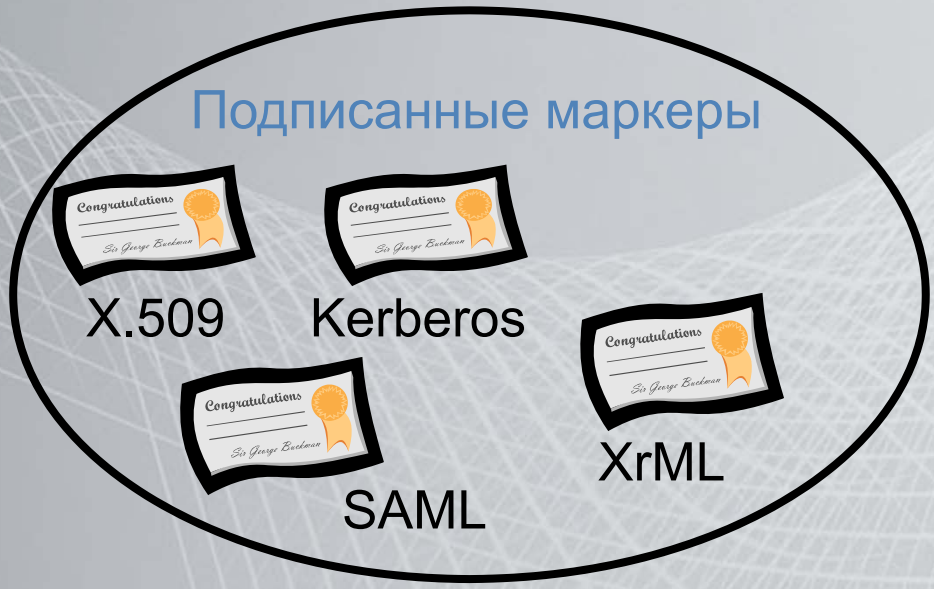
Обмен заявками между организациями/системами

Маркеры безопасности и заявки

Распределенная аутентификация/авторизация

Маркер безопасности включает в себя одну или несколько заявок

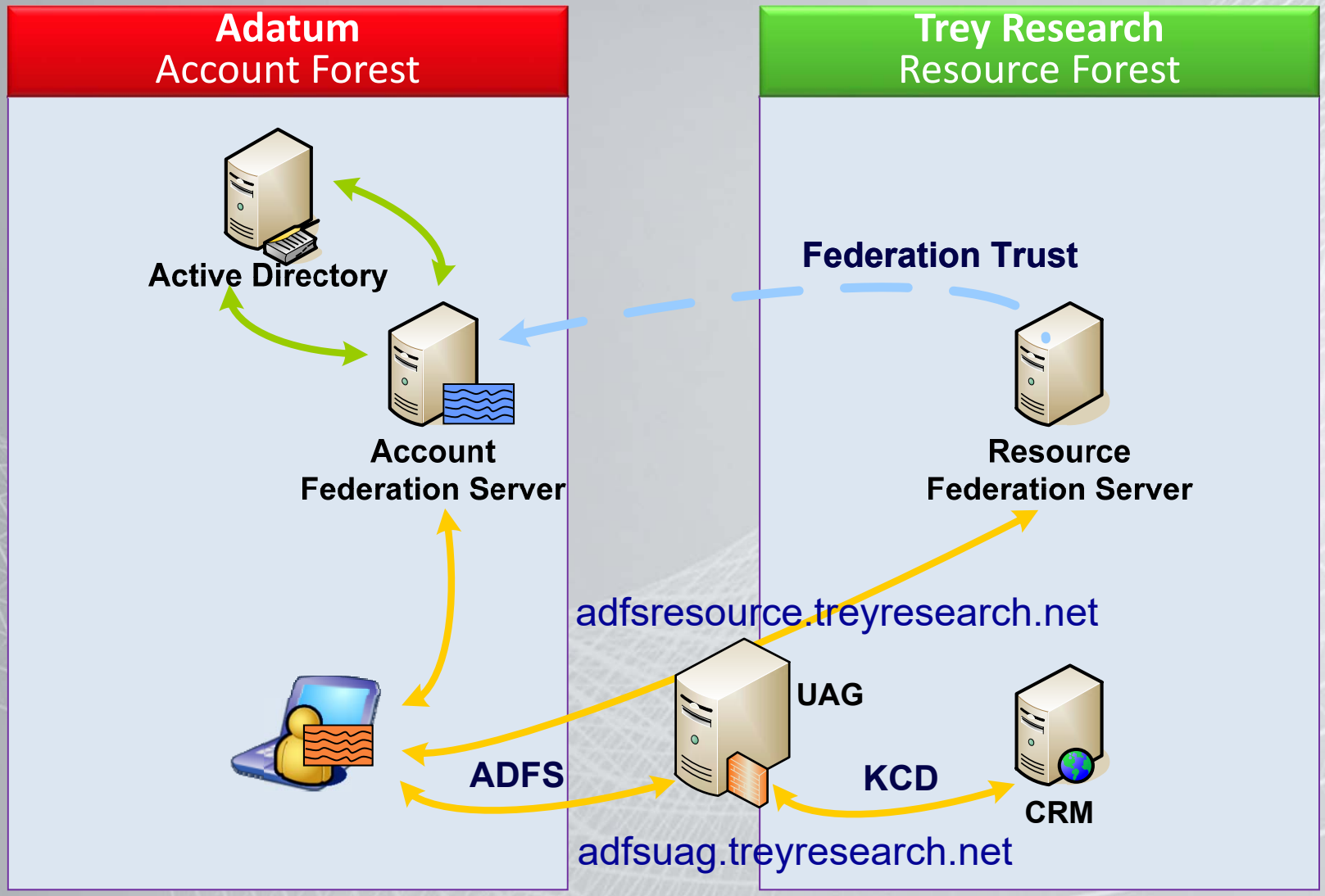
Заявка (Claim) – информация о субъекте безопасности (имя, идентификатор, группа, роль и пр.)



Типы заявок

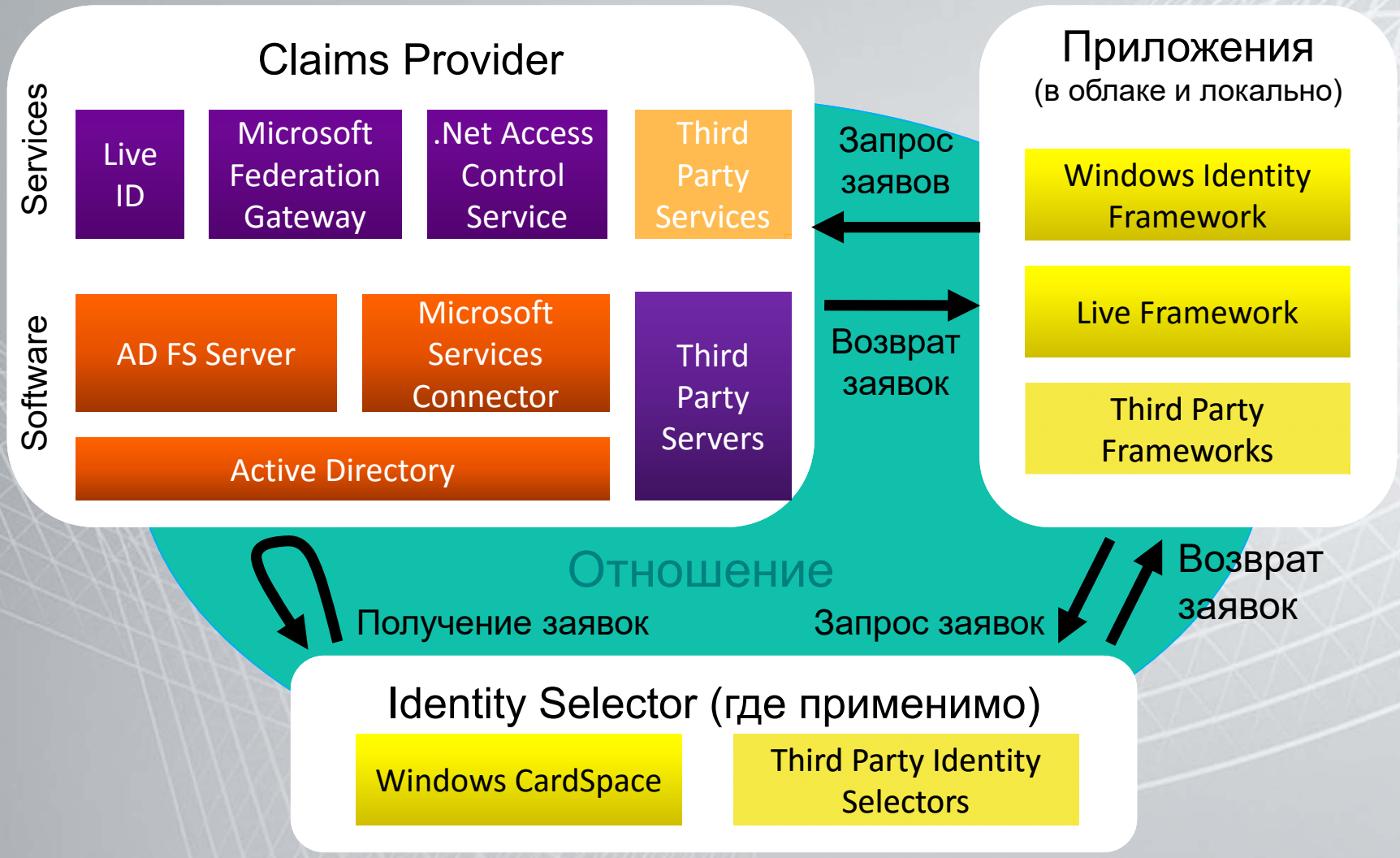
- *Заявка (claim) – заявление одного субъекта о другом субъекте*
- Стандартные типы заявок
  - Идентификатор
    - Email = kcameron@microsoft.com
    - Age > 21
    - Employer = Microsoft
  - Роль/Группа
    - Role = Architect
  - Настраиваемая
    - Пара имя/значение (например, SSN/123-45-6789)
- Организационные заявки
  - Общий набор заявок для хранилищ учетных записей и партнеров
  - Настройка заявок на аудит/протоколирование

Принцип работы ADFS



Identity Software + Services

AD Federation System и модель заявок



sandBox.netFx3.com - Windows Internet Explorer

http://sandbox.netfx3.com/

Live Search

sandBox.netFx3.com

Page Tools

sandBox.netFx3.com

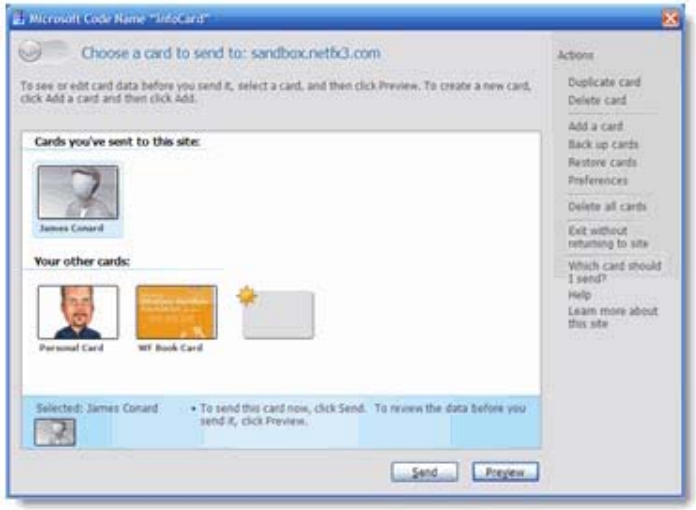
Come and play with Windows CardSpace in the Sandbox!

Welcome to sandBox.netFx3.com Sign in | Join | Help

SEARCH

Home | Blogs

Welcome to the Sandbox - Works with .NET 3.0 RTM and RC1 or later!



What is the Sandbox?

The Sandbox is an area of the NetFx3.com site that has been designed to demonstrate the use of Windows CardSpace. Like most sites on the web today, this site provides the ability to login using a username and password. However, this site has been customized to also use Windows CardSpace for authentication. On the Sandbox site you can:

- Create a user account using a username and password or using a self-issued Windows CardSpace Information Card
- Link one or more Information Cards with your user account
- Sign-in to the site using your username and password or an Windows CardSpace Information Card that you have linked with your account

Microsoft .net Framework

- NetFx3 Home Page
- Windows Communication Foundation
- Windows Presentation Foundation
- Windows Workflow Foundation
- Windows CardSpace

Sandbox Blog

Last updated: 09-05-2006

Done

Internet | Protected Mode: On

100%

sandBox.netFx3.co...

Fabrikam Friends - ...

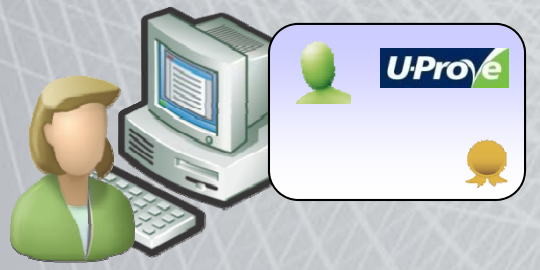
9:35 PM

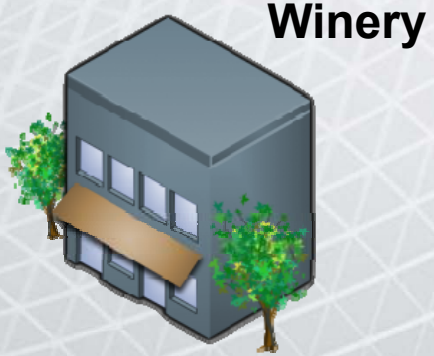
Технология U-Prove

- Криптографическая технология, разработанная в начале 90х
- Позволяет формировать метки

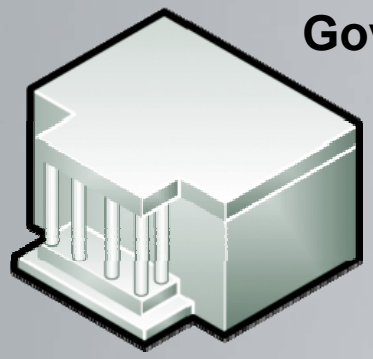
- Метки U-Prove используются для обмена информацией, строгой аутентификации и цифровой подписи
- Имеют ряд уникальных отличий от общепринятых меток безопасности (X.509, SAML, Kerberos)

Минимальное раскрытие



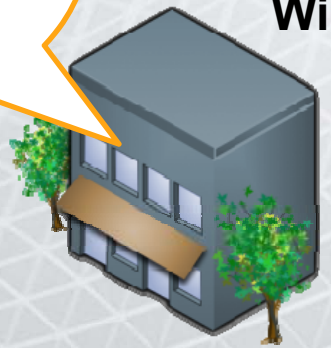


Minimal disclosure

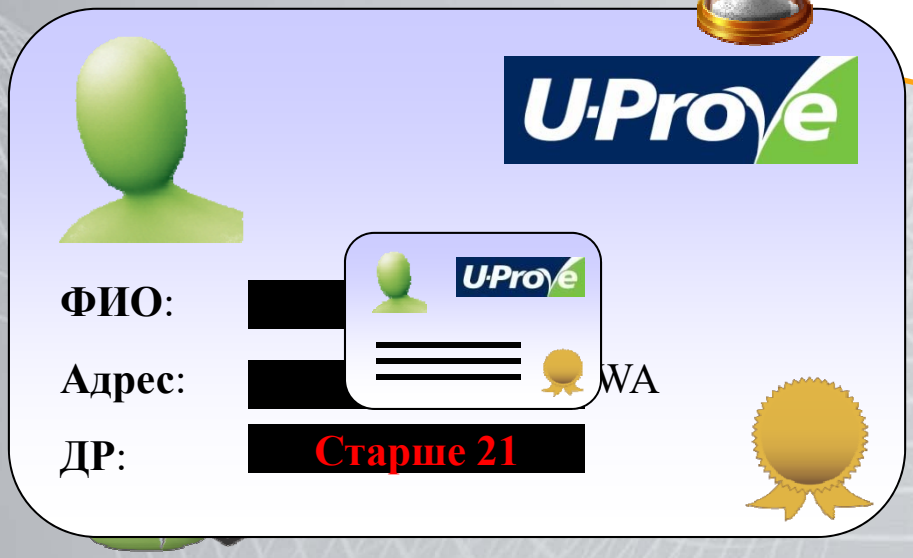


Gov

Докажите, что вам больше 21 и вы из WA



Coho Winery



Вопросы

Алексей Голдбергс
i-alexg@microsoft.com
http://blogs.technet.com/securityrus
Microsoft Россия