



INFORMATION TECHNOLOGY SERVICES

Web Services Security KPMG LLP Case Study

ITS US APPLICATIONS

Securing and Managing a Web services Environment

◆ Goals for this session

- What were our challenges?
- What was our solution?
- What is the status of key enabling standards?

Who is KPMG

◆ KPMG LLP Profile

- Multi-National presence
- Decentralized model
- Large Microsoft User
- Disparate technology base
- Desire for a common application platform

Opportunity: Architecture Consolidation

- ◆ Reduce costs for development, support and maintenance by introducing a services framework with strong reuse capabilities
- ◆ Orchestrate convergence of various IT initiatives around common standards of performance and connectivity
- ◆ Improve ability to adapt/respond quickly and be flexible to changing business conditions
- ◆ Provide a platform that enables consistent delivery of new technologies

Design Principles of Application Platform

◆ Technical criteria

- Integrates with Single Sign-on Infrastructure
- Exposes Web Services
- Can be extended using .Net Framework

◆ Single Infrastructure

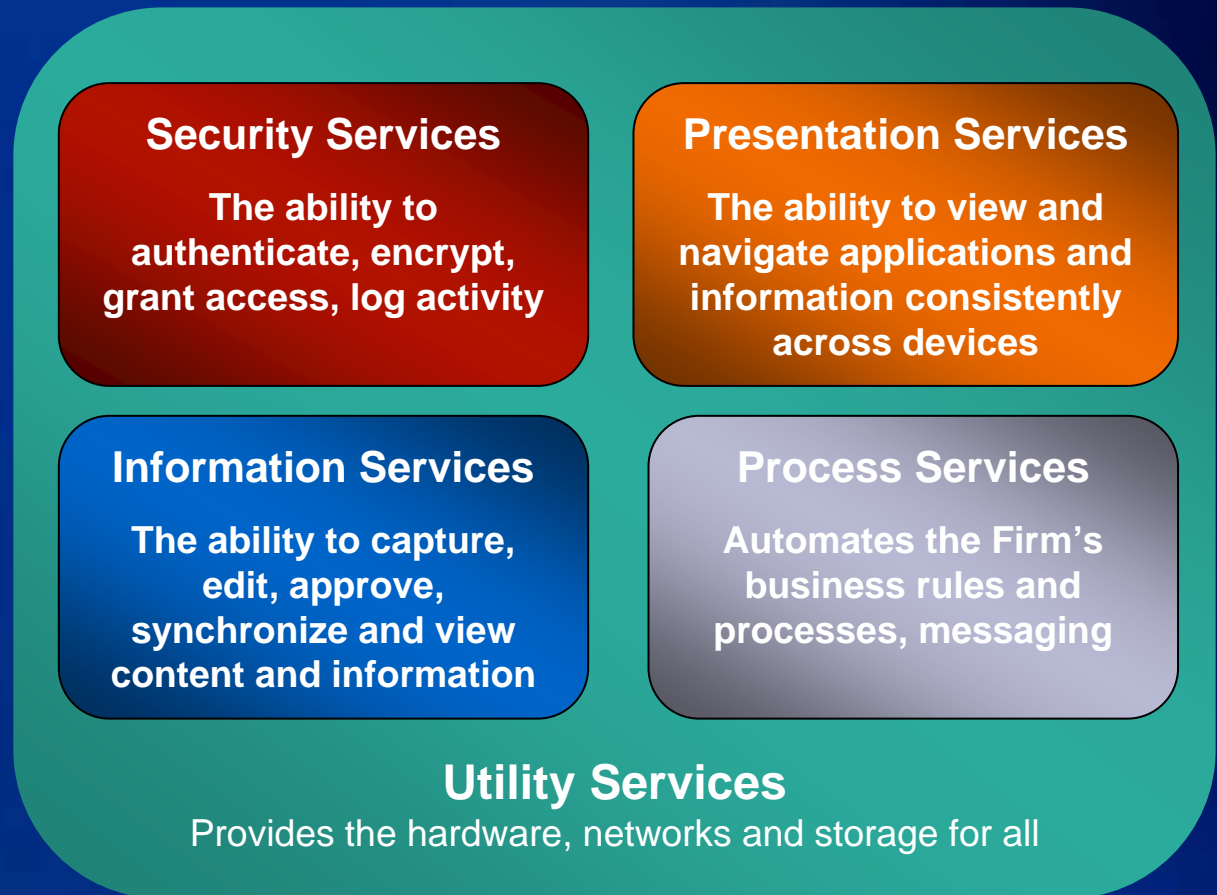
- Supports both internal and external use

◆ Distinct Non-Trusted Domain

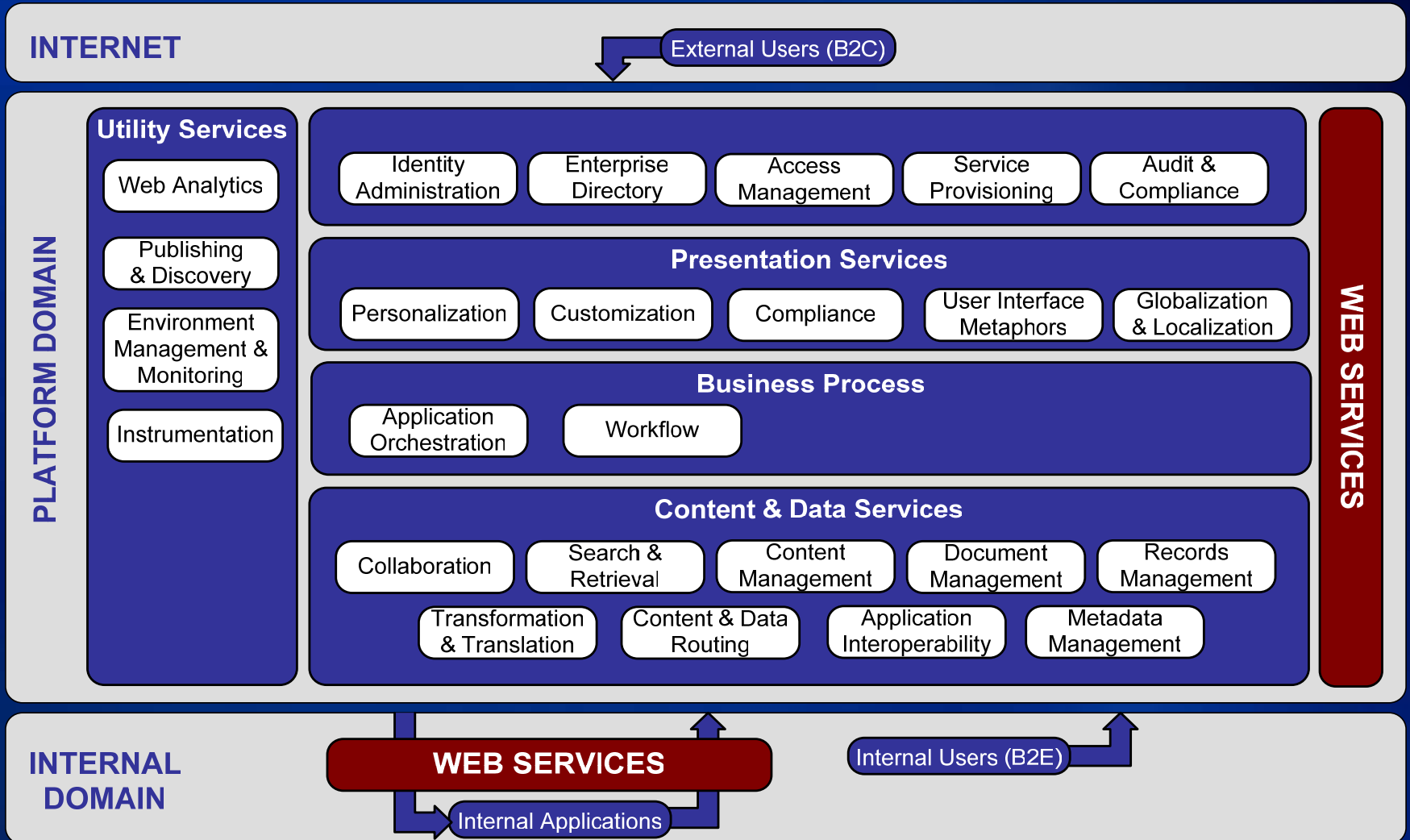
- Separate from internal network and internet

Application Platform Concept

- ◆ Delivers capabilities spanning the five core services of the firm's application architecture:
 - Security Services
 - Presentation Services
 - Process Services
 - Information Services
 - Utility Services
- ◆ Capabilities are then combined to deliver business solutions



Solution: Application Platform



What were our Web Services Requirements

- ◆ Technical
- ◆ Security
- ◆ Operational

Technical Requirements

- ◆ Retrieval and/or manipulating information.
- ◆ Enable application to application communication.
- ◆ Publish and discover web services.
- ◆ Architect with Performance in mind.

Security Requirements

- ◆ Accessible over SSL (port 443) only
- ◆ Authentication provided by Single Signon environment
- ◆ Compliant with Internal KPMG Security policies
- ◆ Web services can operate behind the firewall and extended to partners and clients
- ◆ Must integrate Web Services with existing security frameworks (i.e. Identity Management and Directory Services)
- ◆ Security standards will be MS compliant (WSE)

Operational Requirements

- ◆ All installed components and configurations must be clearly documented with information on how to troubleshoot possible problems
- ◆ Web services and clients must report serious errors to the appropriate sink
- ◆ Web services for public consumption must have SLA's

Security Challenges

Security Challenges

- ◆ Security standard for Web Services (i.e. WS-Security) are emerging however they have not been widely adopted
- ◆ Most implementations utilize either custom security layers or vendor specific approaches like Microsoft's Web Services Extensions (WSE)
- ◆ Trust models for secure Web Services transactions over the internet are immature

Operational Challenges

Operational Challenges

- ◆ Existing support processes are not directly applicable to distributed Web Services architectures
- ◆ Governance models for Web Services architectures are immature
- ◆ Few tools exist that provide end-to-end management for distributed, Web Service based applications
 - Trouble shooting
 - Performance monitoring
 - SLA compliance
 - Capacity planning

Web Services Approach

Considerations

- ◆ **We made a distinction between Web Services and SOA:**
 - SOA is a design and architecture principle
 - Web Services is a physical implementation of an SOA approach
 - Web Services can exist without SOA
- ◆ **An application must be Web Services capable:**
 - Many applications cannot handle the unexpected traffic
- ◆ **PKI would be nice but:**
 - It is a very expensive proposition

Web Services Design Guidelines

◆ Two Types of web services

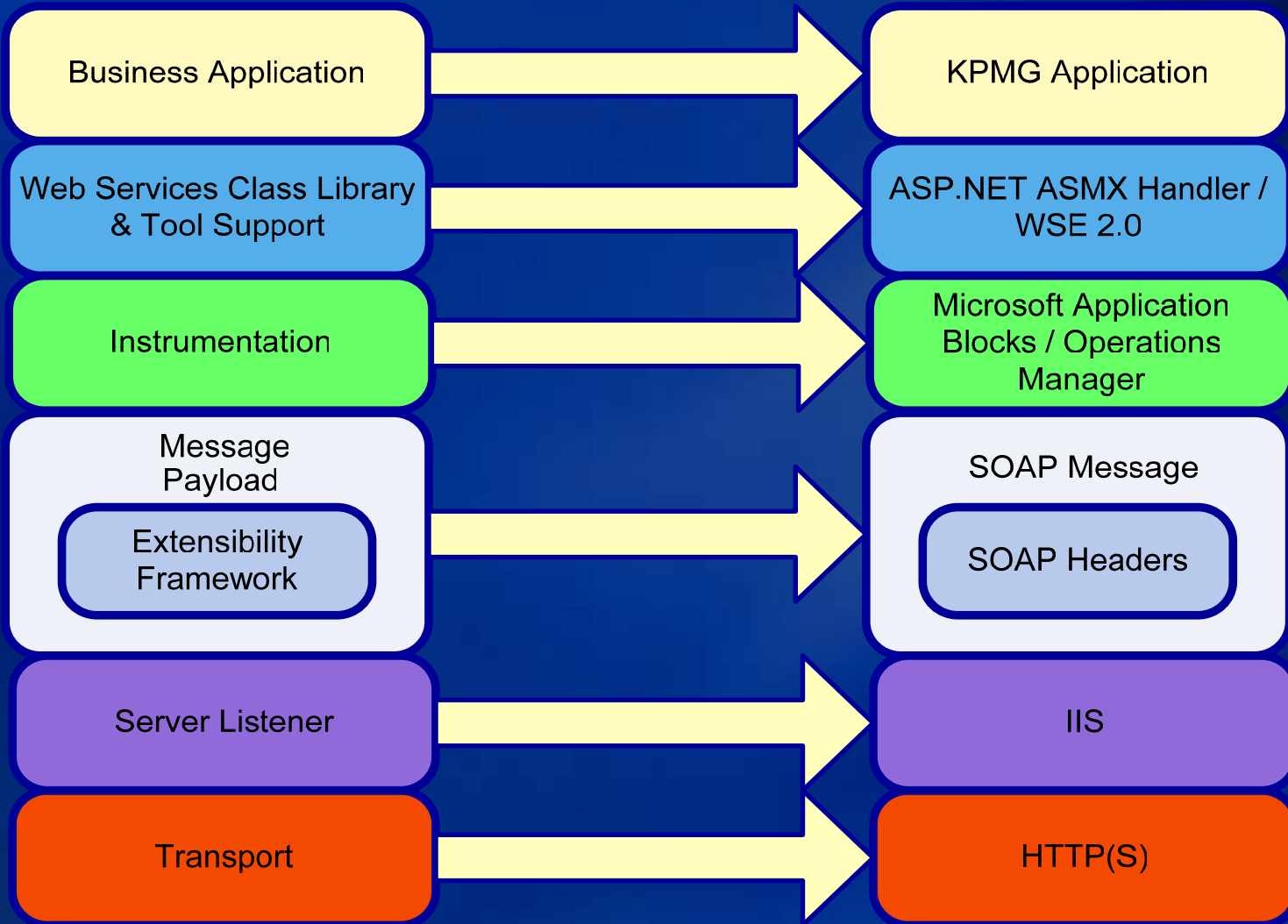
– Point to Point

- Database access
- Single data point retrieval
- CRUD

– Business process or functionality

- Built around a specific process (Get Client etc.)
- Encapsulates business logic within the Web Service

Web Services Stack



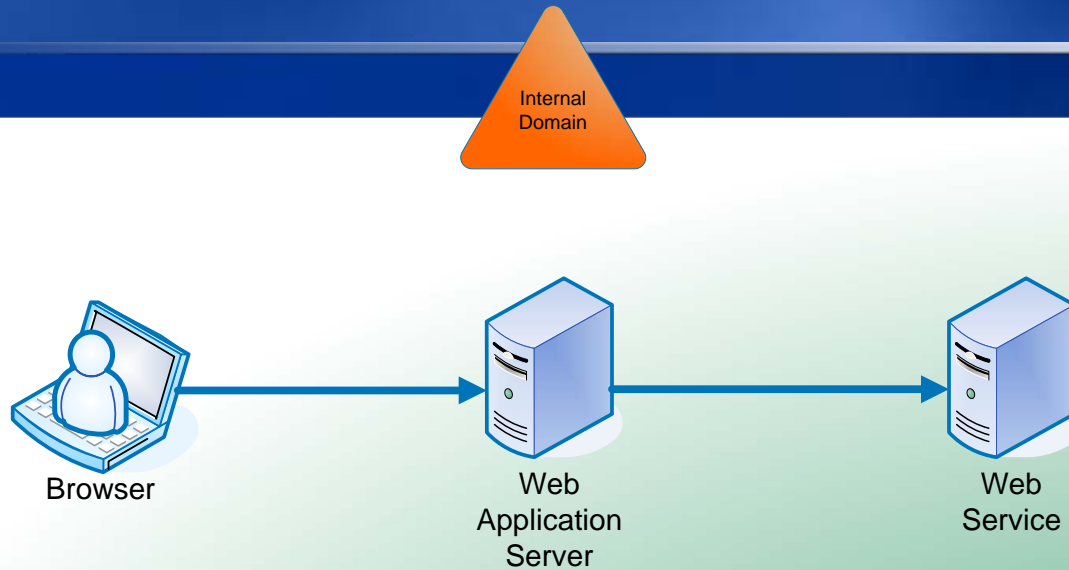
4 Primary Use Case

- ◆ **Internal Web Service**
- ◆ **Accessing a Web Service on the Application Platform**
- ◆ **Round Trip access to a Web Service**
- ◆ **Service Account access to a Web Service**

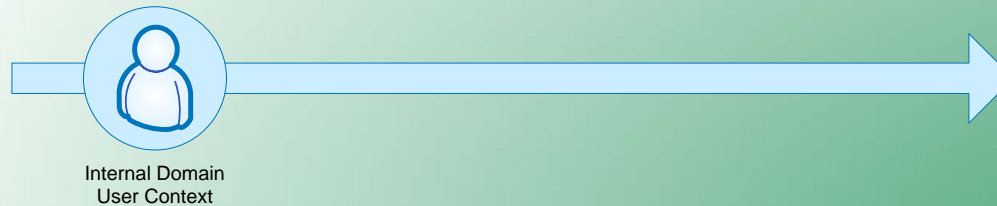
Web Services Security Approach

- ◆ **Ensure proper recipient**
- ◆ **Guarantee identity across all trust barriers**
- ◆ **Utilize WSE**
 - Provides framework for Passing Credentials
- ◆ **Exploit KPMG Single Sign-on environment**
 - Provides a mechanism to supply user and role info
- ◆ **Utilize HTTP/S to pass credentials**
 - Supporting both user and service accounts

Internal Web Service

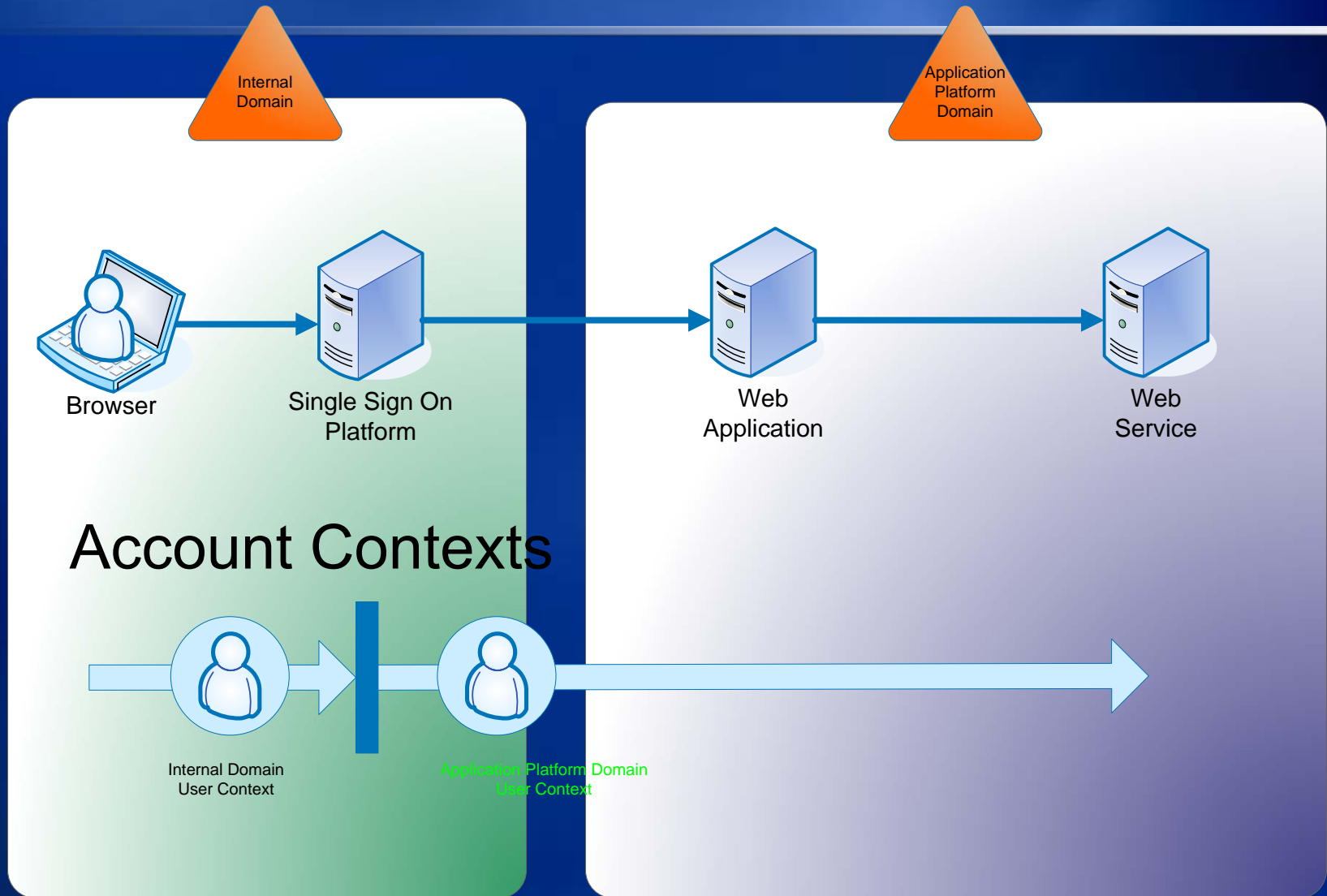


Account Context



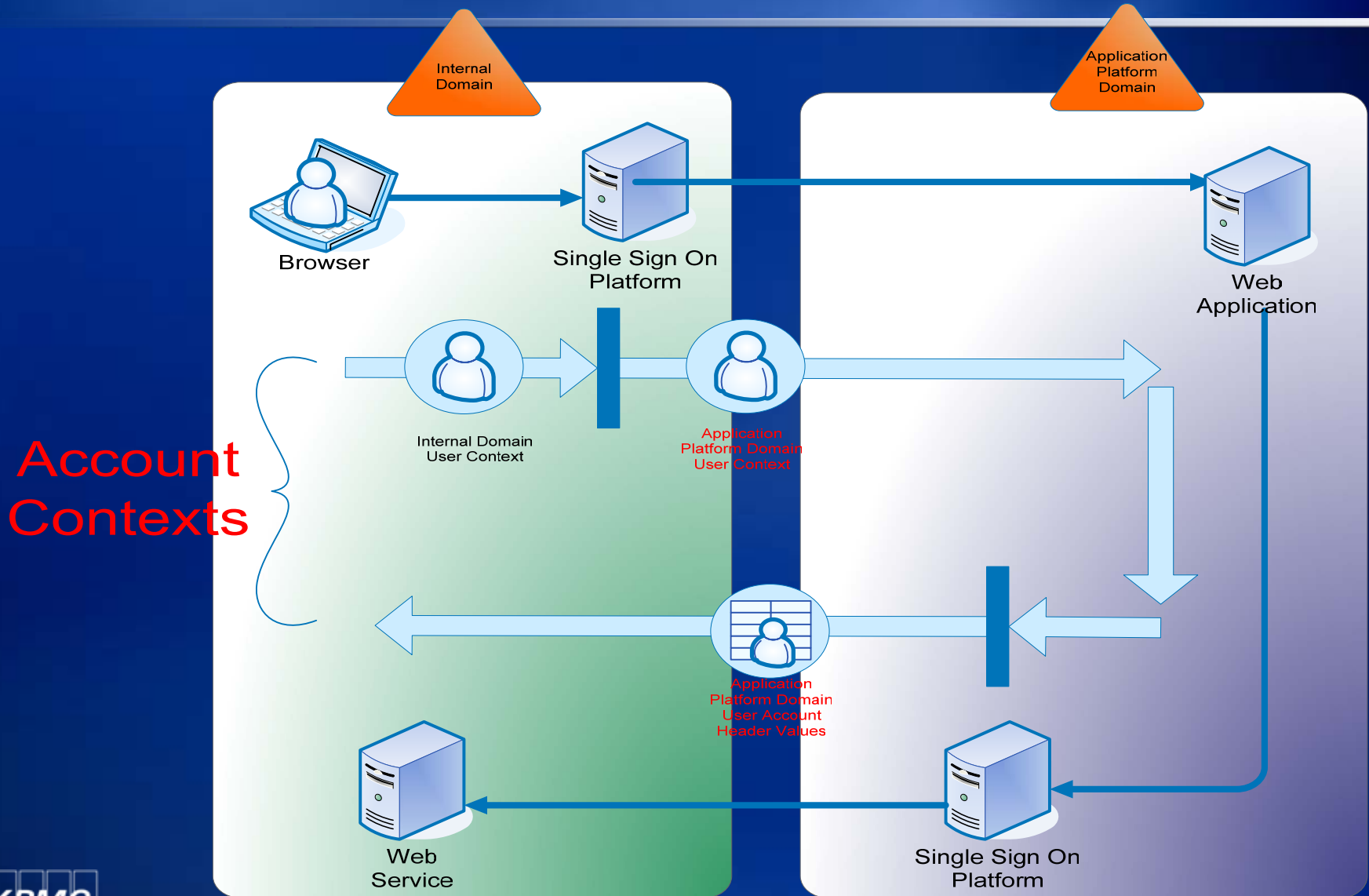
IIS, Kerberos, and Active Directory are sufficient for proving the identity of the caller.

Accessing Web Services on Application Platform

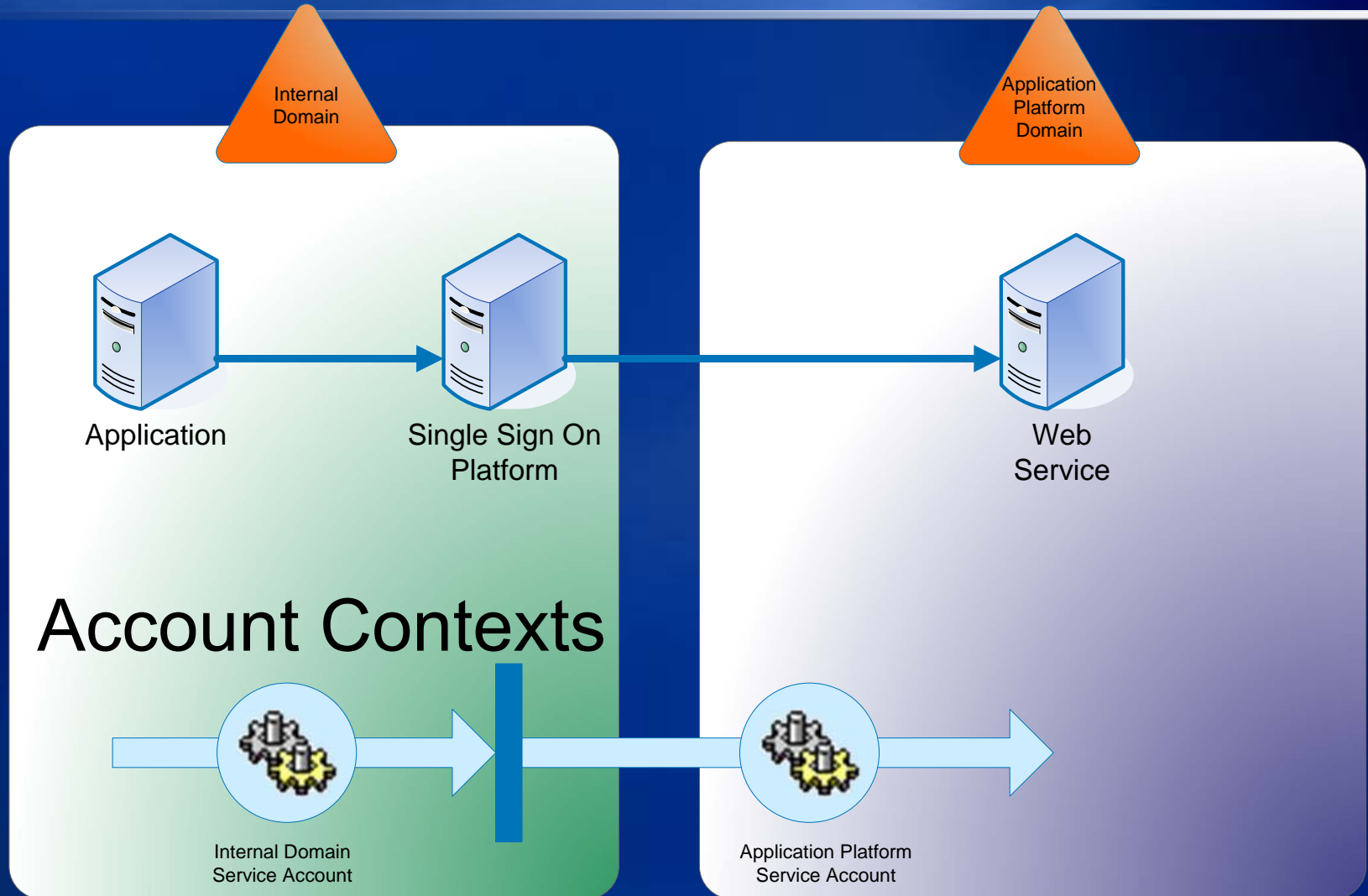


Account Contexts

Round Trip Access Internal to External



Service Account Access to Web Service



On the Horizon

- ◆ **WSE 3.0 – Find out what it will add**
- ◆ **UDDI**
- ◆ **Web Services Management**
 - Performance
 - SLA
- ◆ **PKI**



Presenter's contact details

Ken Shea

KPMG LLP

kshea@kpmg.com

www.kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.