



INFORMATION TECHNOLOGY SERVICES

# Web Services Security

## KPMG LLP Case Study

ITS US APPLICATIONS

# Delivering and Managing a Web services Environment

## ◆ Goals for this session

- What were our challenges?
- What was our solution?
- What are future consideration?

# Who is KPMG

## ◆ KPMG LLP Profile

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

# Opportunity: Consumption & Flexibility

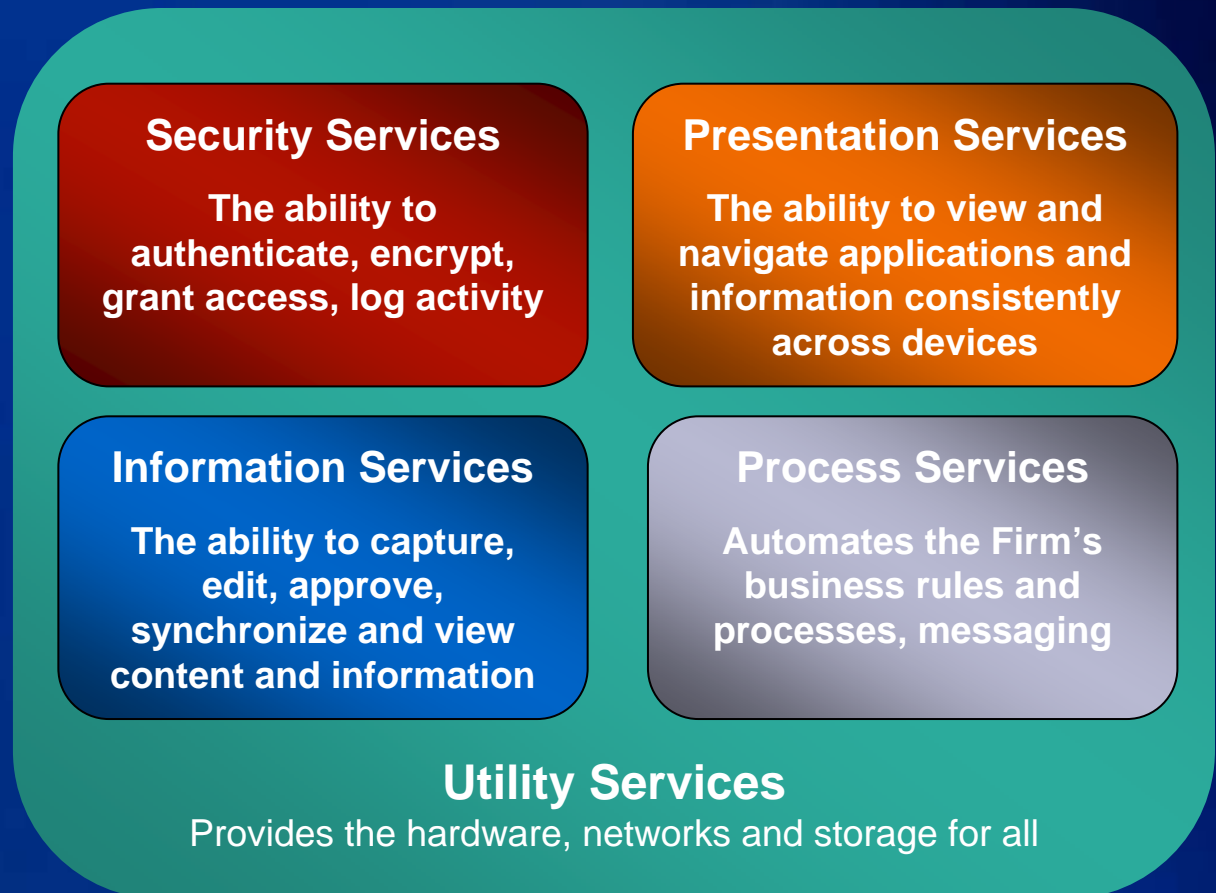
- ◆ Reduce cost of integration for application
- ◆ Turn middleware capabilities into a service
- ◆ Begin to use web services as a design paradigm
- ◆ Validate assumptions about our common platform

# Application Platform Concept

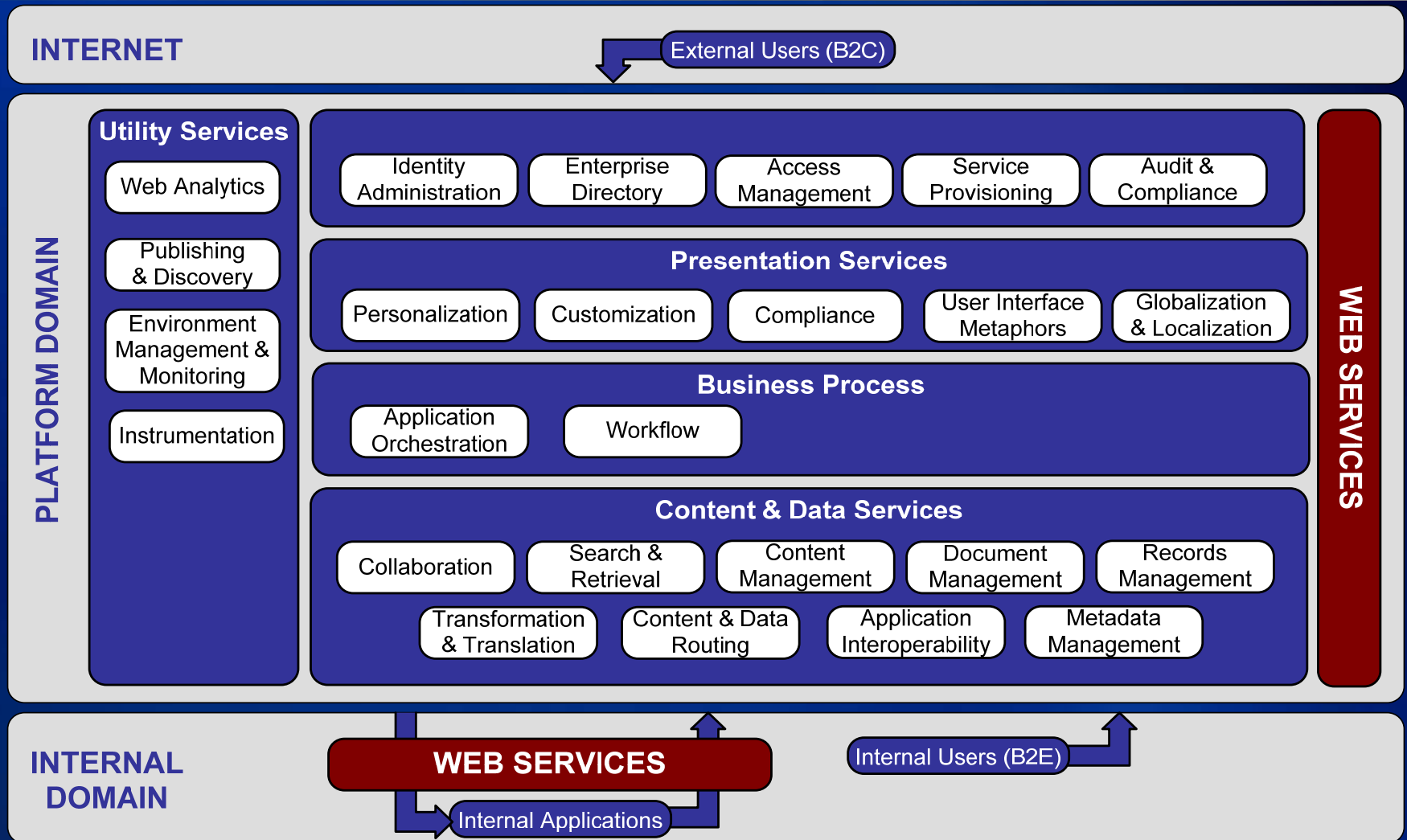
- ◆ Delivers capabilities spanning the five core services of the firm's application architecture:

- Security Services
- Presentation Services
- Process Services
- Information Services
- Utility Services

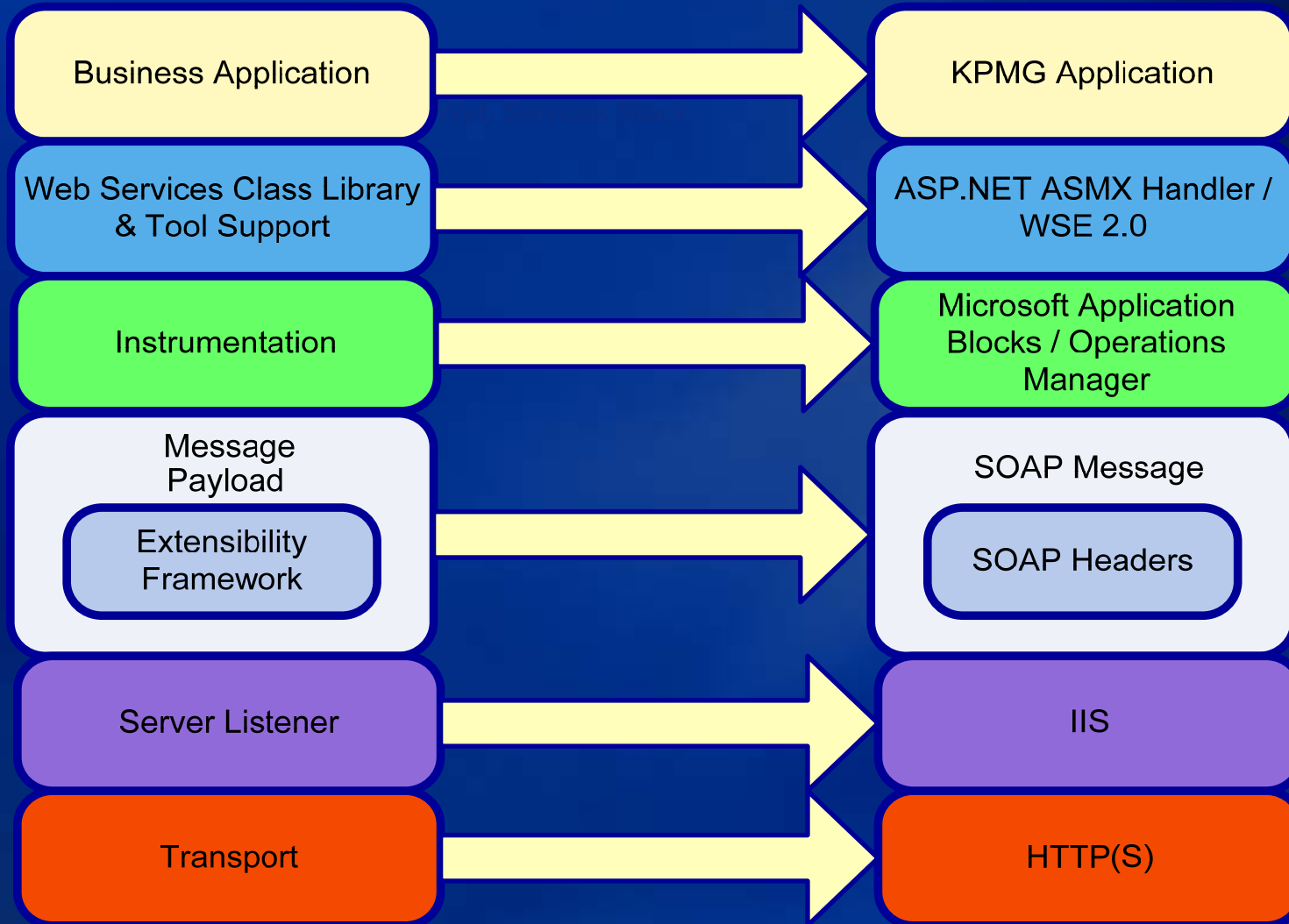
- ◆ Capabilities are then combined to deliver business solutions



# Solution: Application Platform



# Web Services Stack



# **Identity Management Web Services**

## **Securing Ourselves**

# Fly our own plane: Identity Management Web Services

## ◆ Authentication:

- Verification of who I am.
  - Showing ID at airport check-in counter.

## ◆ Authorization:

- What can I do
  - I can get on the plane, but can I use the first class lounge

## ◆ Auditing:

- What have I been doing lately
  - What did I do when I used the first class lounge.

# Project Objectives

- ◆ **Create a Web Service for Identity Management:**
  - Consistent integration across the application houses.
  - Centralized security solution for data access and management of protected resources.
  - Improved auditing of protected data.
  - Enhanced security.
- ◆ **Enable applications to manage their own security.**
  - Groups
  - Profiles

# Before and After

	Current State		Future State
✓	Decentralized API solution.	✓	Centralized solution. No client footprint.
✓	Required a client instal	✓	No installation on client.
✓	24 hour turnaround for change requests.	✓	Real time updates to add and remove users. Applications can manage their own security.
✓	Difficult to manage multiple versions of the APIs for clients.	✓	Platform independent. Generalized services that accommodate .Net and JAVA.
✓	Client invokes local APIs.	✓	Better Security.
		✓	Easier support.

# Web Service Considerations

# Web Services Considerations: Technical

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

# Web Services Considerations: Security

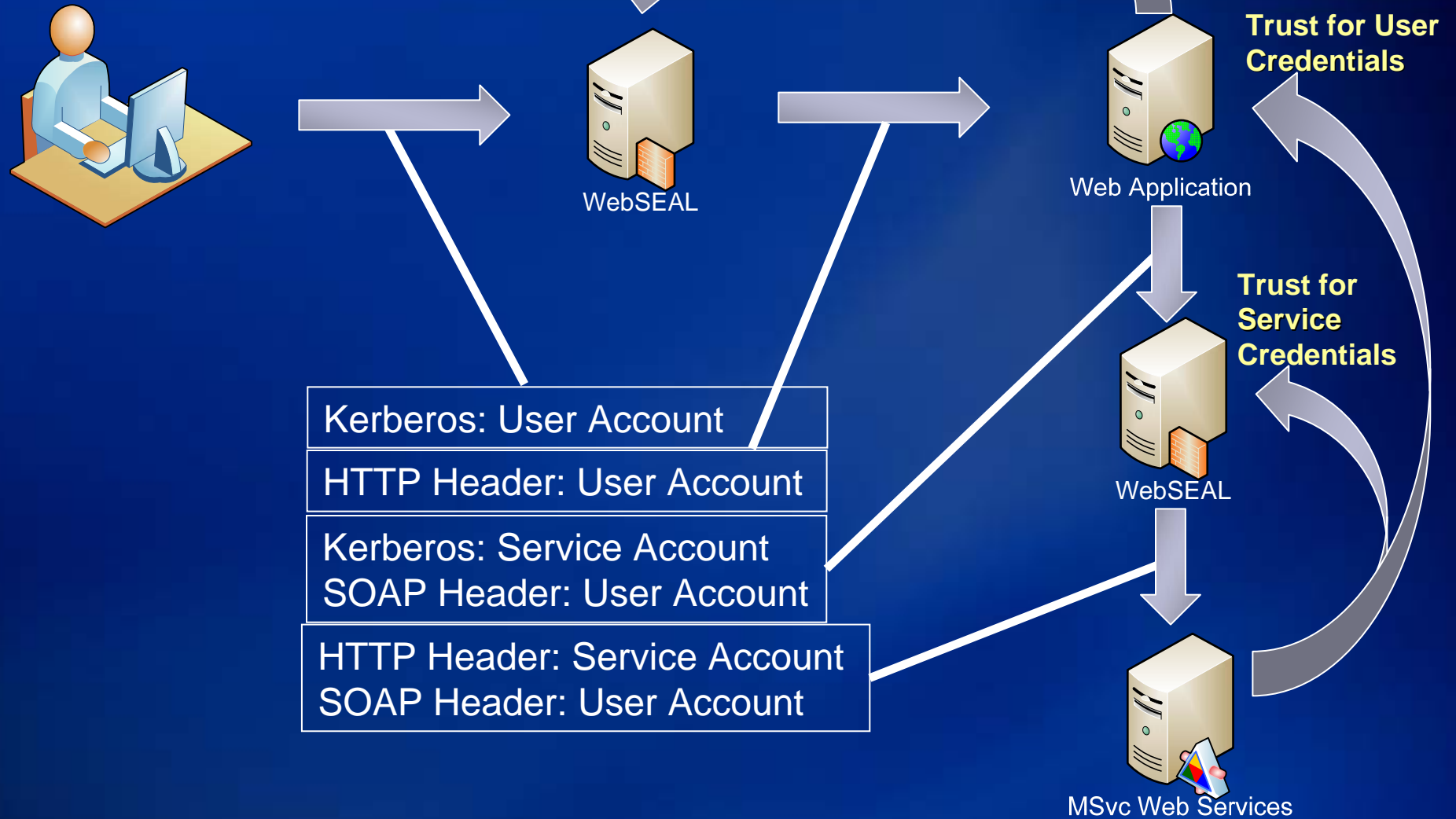
- ◆ Accessible over SSL (port 443) only
- ◆ Authentication provided by Single Signon environment
- ◆ Compliant with Internal KPMG Security policies
- ◆ Web services can operate behind the firewall and extended to partners and clients
- ◆ Must integrate Web Services with existing security frameworks (i.e.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

# Web Services Considerations: Operational

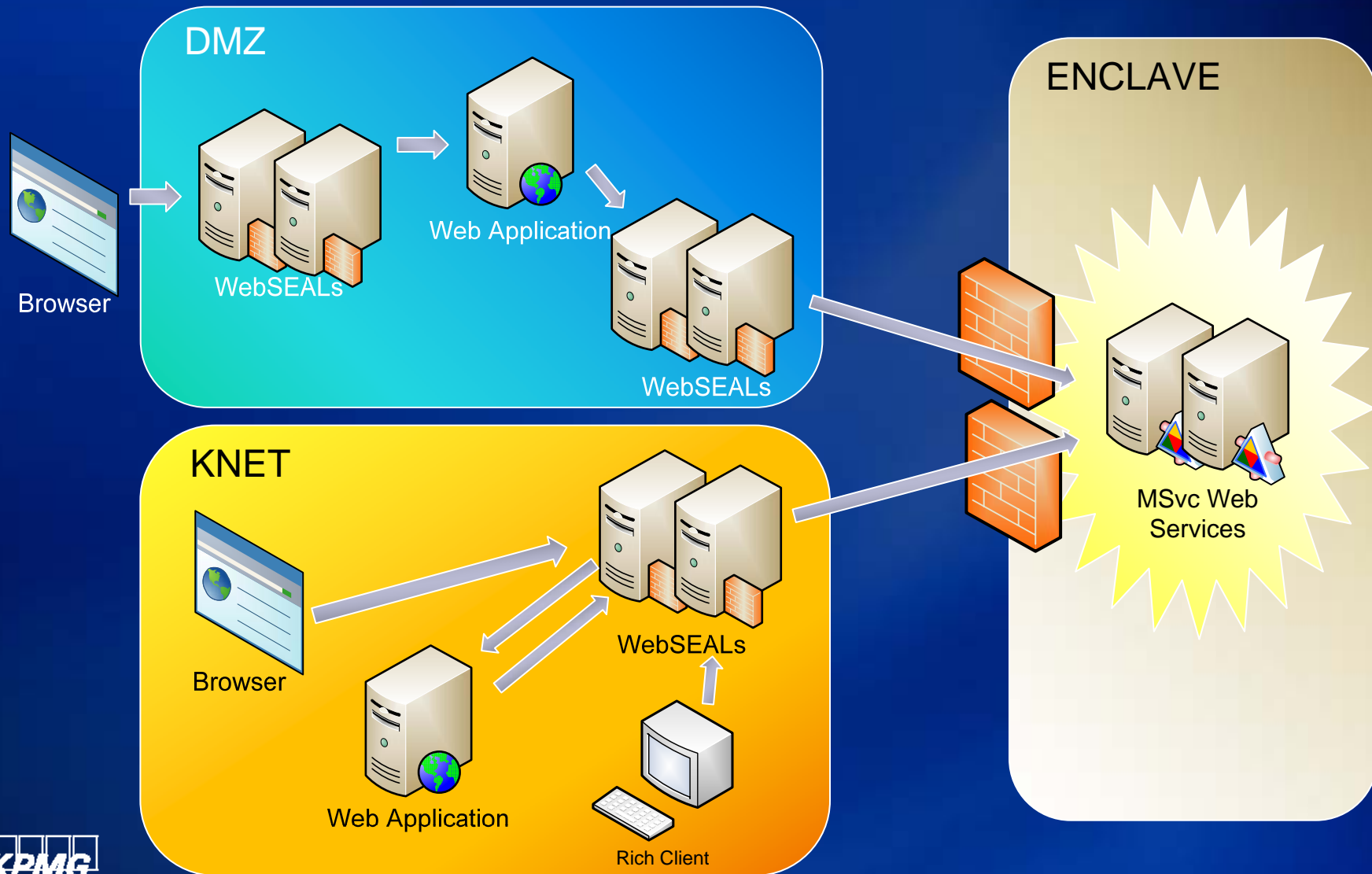
- ◆ All installed components and configurations must be clearly documented with information on how to troubleshoot possible problems
- ◆ Web services and clients must report serious errors to the appropriate sink
- ◆ Web services for public consumption must have SLA's

# Web Services Architectural Design

# Web Service Authentication



# Production Environment



# Web Services Challenges

# Challenges: Security

- ◆ **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**

# Challenges: Operational

- ◆ **Scalability of a web service infrastructure**
  - Load Balancing
  - Management and complexity
- ◆ **Versioning control**
- ◆ **Error Messaging in the event of failure**
- ◆ **Policy Governance**
  - How does one get access
- ◆ **Policy Enforcement**
  - Permission based on your access

# Management Alternatives

## ◆ Appliance

- DataPower

## ◆ Software

- AmberPoint
- Systinet
- Microsoft



## **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.