您的潜力，我们的动力

Microsoft
微软（中国）有限公司

Windows Communication Foundation 的安全体系架构

徐栋
北京中达金桥技术服务有限公司
xudong@itgoldenbridge.com

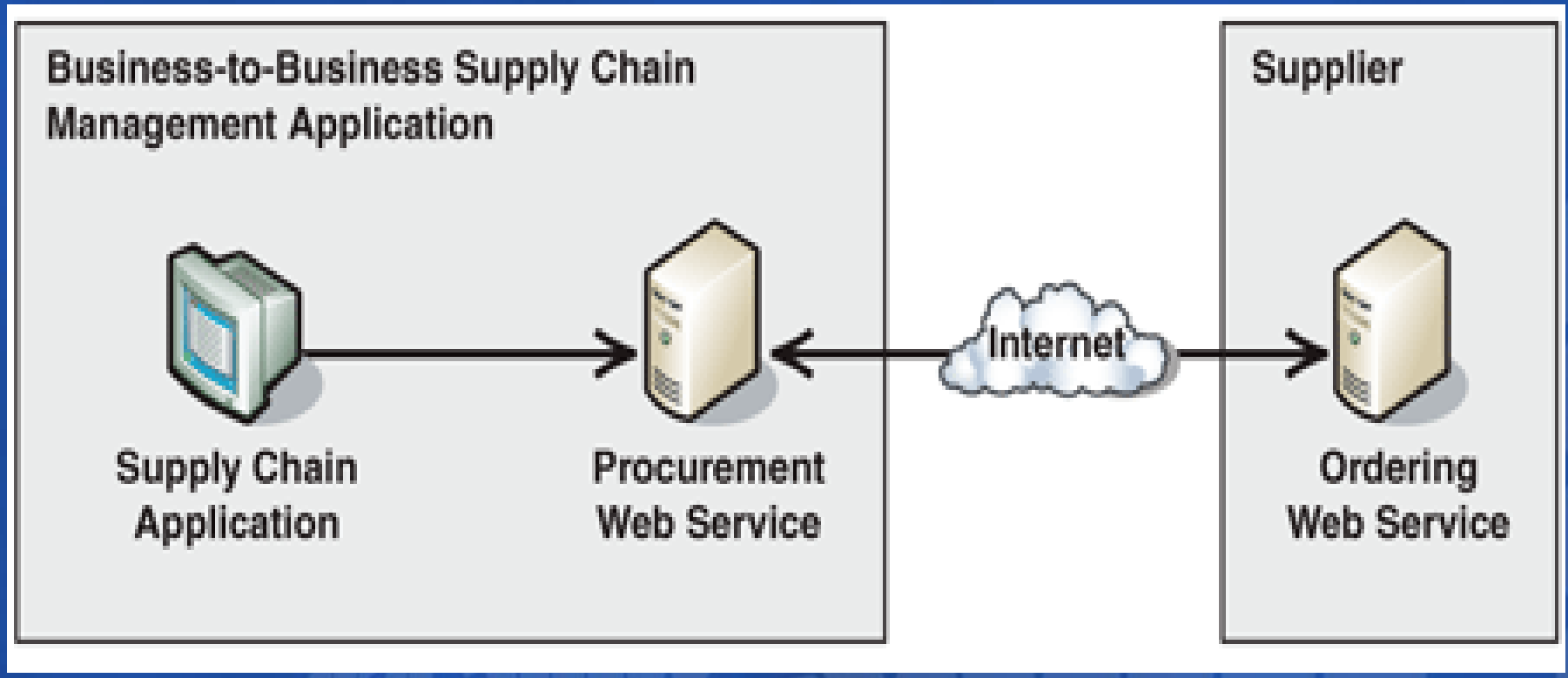
msdn

MSDN Webcasts

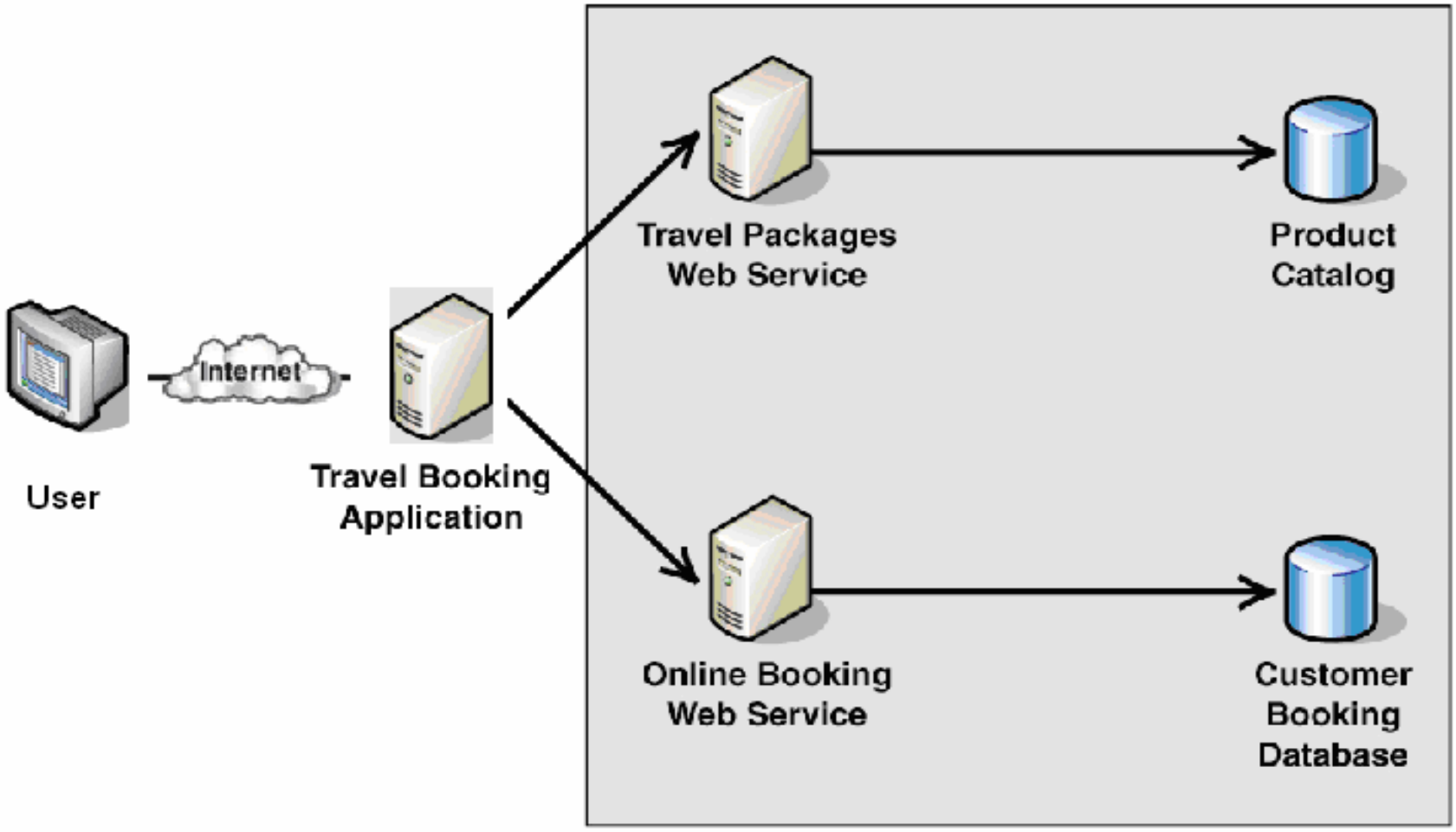
议程

- 分布式应用的安全要素
- **WCF**安全系统模型
- 演示
- 问答

应用场景1:
供应链采购系统（B2B）



应用场景2:
在线旅游服务系统（B2C）



分布式应用的安全要素

- 机密性(Confidentiality)
- 完整性(Integrity)
- 认证(Authentication)
- 授权(Authorization)
- 审计(Auditing)
- 身份(Identity)
- 凭证(Credential)

机密性及完整性

- 数据别人能否偷看到？传输过程中有没有篡改过？

身份及凭证

- 你是谁？如何证明你就是这个人？

Alice — Username

MyDomain\Alice — Kerberos

Subject: CN=Don Box
Issuer: Microsoft Corp CA
ValidFrom: 2005-09-13
ValidUntil: 2006-09-16 — Certificate

认证

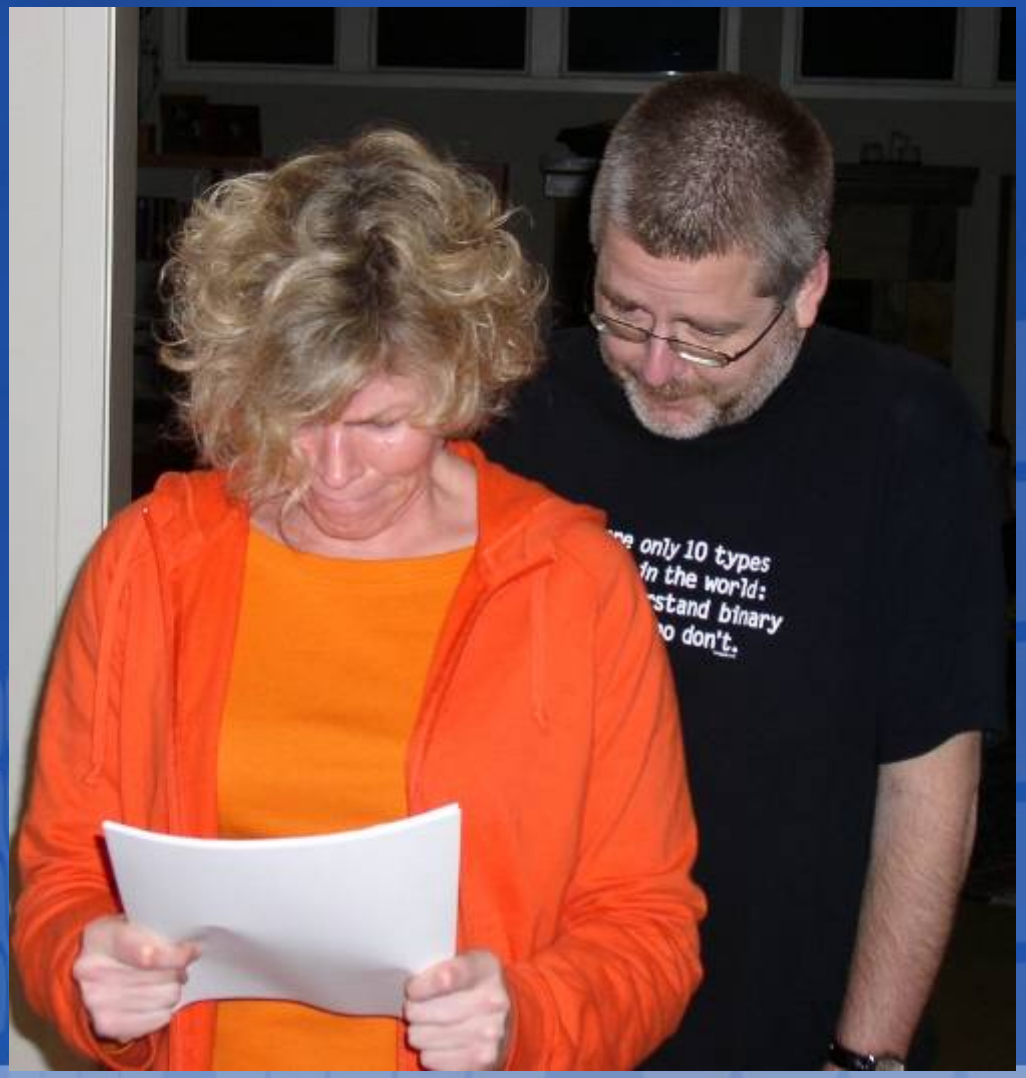
- 你真的是这个人吗？

授权

- 你能干什么？

审计

- 你干了些什么



WCF安全系统模型

- 解决的问题：
  - 保证消息在传输过程中的安全（机密性及完整性）
  - 保证资源访问的安全
- 可通过配置或代码实现
- 缺省配置是安全的

保证数据在传输过程中的安全

- 保证机密性：加密
- 保证完整性：数字签名
- 两种模式：传输层（**Transport**）或消息层（**Message**）层
  - 也可使用混合模式
- 两个级别：仅签名或加密+签名
- 通过**Binding**上的设置来实现

```
<basicHttpBinding name="BasicHttpBinding">
  <binding>
    <security mode="Message">
      <transport clientCredentialType="Basic"
                 proxyCredentialType="Windows" realm="myrealm.com"/>
      <message clientCredentialType="Certificate" algorithmSuite="Aes128"/>
    </security>
  </binding>
</basicHttpBinding>
```

传输层的数据安全

- 在传输（协议）层进行安全保护
- 优点：
  - 速度更快
  - 传输层安全技术在业界已有广泛的采用
- 缺点：
  - 只能使用少数凭证（**Credential**）机制
  - 数据在脱离转输管道后，就不再受到保护

传输层的数据安全（续）

```
<endpoint address="https://localhost/calculator"
                    binding="basicHttpBinding"
                    bindingConfiguration="Binding1"
                    contractType="ICalculator" />


<basicHttpBinding>
      <binding configurationName="Binding1">
          <security mode="Transport">
              <transport clientCredentialType="None"/>
          </security>
      </binding>
</basicProfileBinding>
```

您的潜力，我们的动力

Microsoft
微软（中国）有限公司

DEMO:
在传输层保证消息的安全

msdn

MSDN Webcasts

消息层的数据安全

- 对数据本身进行加密，与传输协议无关
- 优点：
  - 支持更多的凭证（**Credential**）类型
  - 可只对选择的部分数据进行加密
  - 提供**End to End**的数据安全机制
  - 可扩展性强
- 缺点：
  - 性能不及传输层加密机制

消息层的数据安全（续）

```
<endpoint address="http://localhost/calculator"
                    binding="wsHttpBinding"
                    bindingConfiguration="Binding1"
                    contractType="ICalculator" />


<wsHttpBinding>
  <binding configurationName="Binding1">
      <security mode="Message">
          <message clientCredentialType="Windows"/>
      </security>
  </binding>
</wsHttpBinding>
```

DEMO:
在消息层保证数据的安全

使用混合模式保护数据的安全

- 是传输层和消息层两种安全模式的折衷
- 传输层：
  - 满足加密及签名等需求
  - 提高性能
- 消息层：
  - 提供丰富的凭证（**Credential**）类型
  - 增强扩展性

使用混合模式保护数据的安全（续）

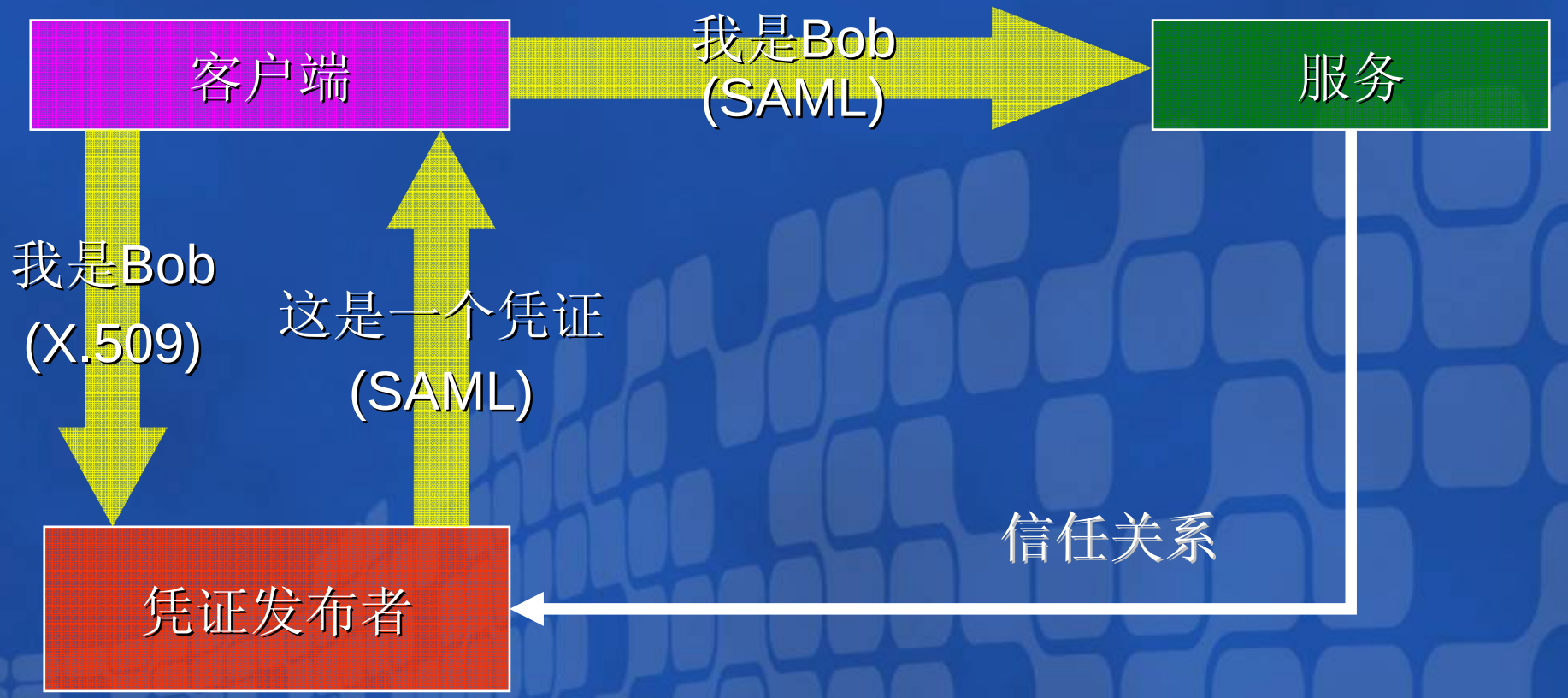

```
<endpoint address="https://localhost/calculator"
                    binding="wsHttpBinding"
                    bindingConfiguration="Binding1"
                    contractType="ICalculator" />


<wsHttpBinding>
  <binding configurationName="Binding1">
      <security mode="TransportWithMessageCredential">
          <message clientCredentialType="Windows"/>
      </security>
  </binding>
</wsHttpBinding>
```

安全会话及统一凭证

- 安全会话（**Secure Session**）
  - 减少认证次数，有助于提高性能
  - 与传输协议无关
  - 通过消息层实现
- 统一凭证（**Federation Credentials)**
  - 由共同信任的第三方发布
  - 支持任意类型的凭证

统一凭证的工作流程

Federated Credentials



保证资源访问的安全

- 多道安全关卡
- 每一道关卡均对相应的权限进行检查并依此批准/拒绝访问

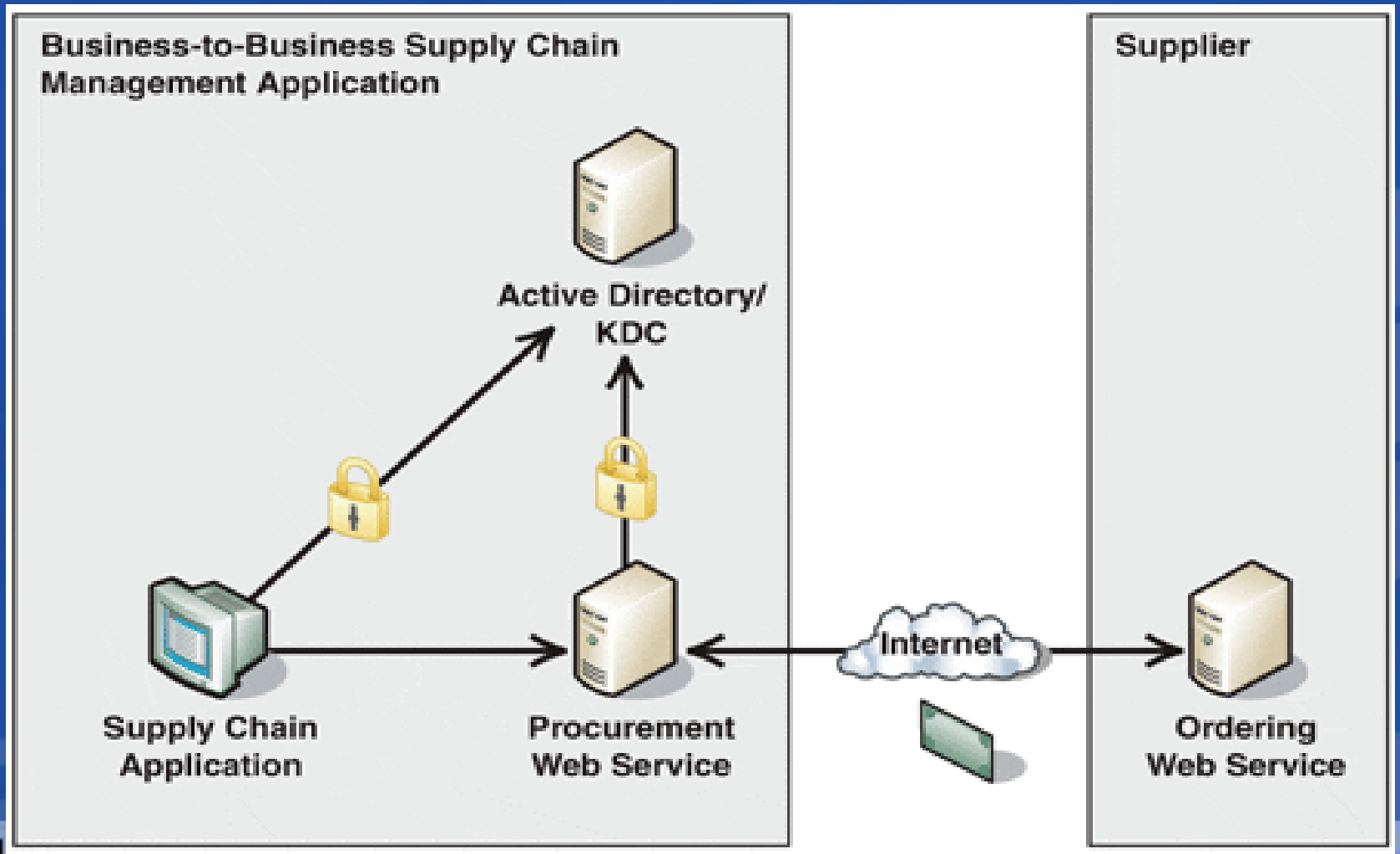
DEMO：保证资源访问的安全

WCF中的安全审计

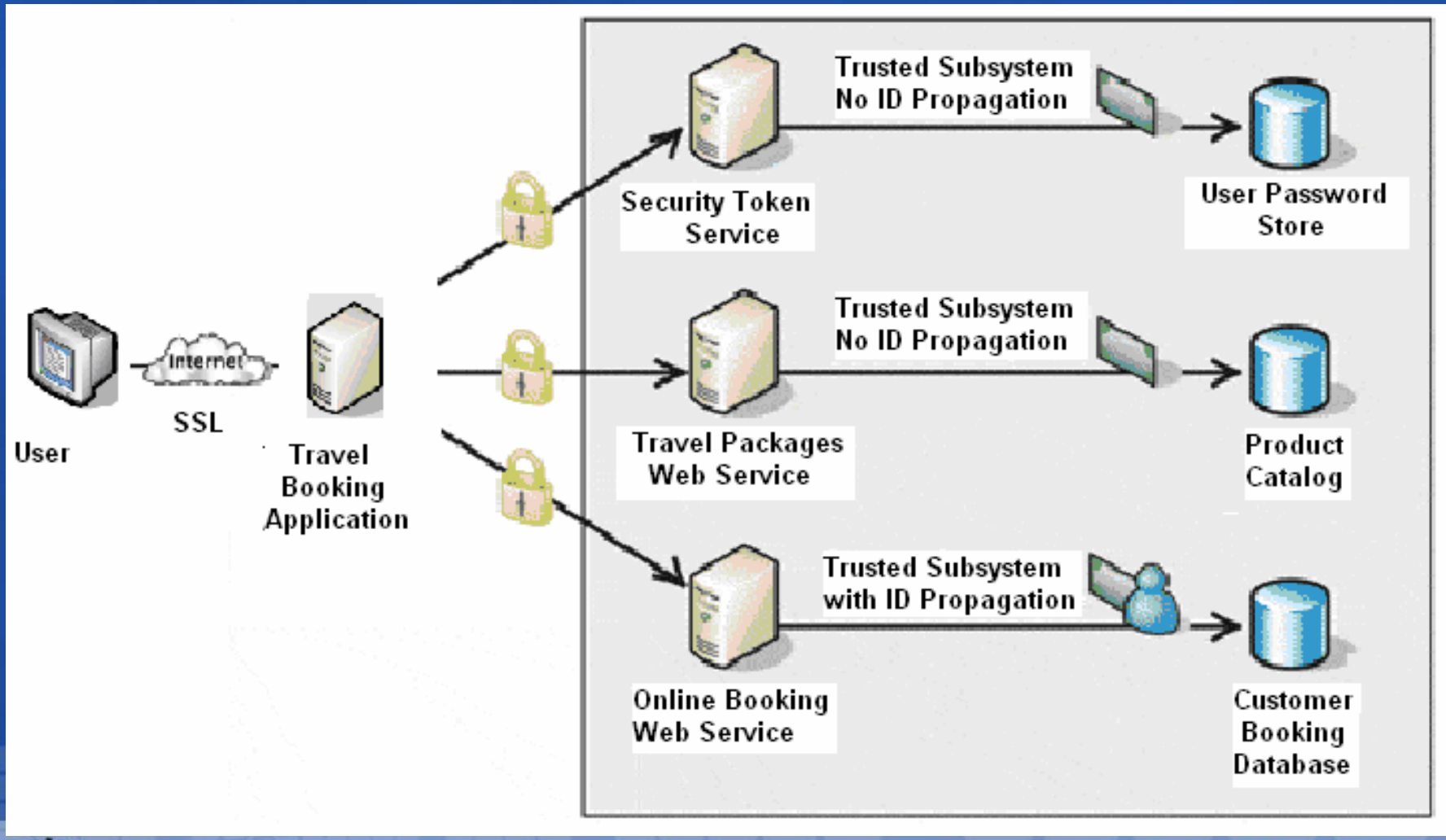
- 安全相关的事件均被记录
  - 应用的起始和结束
  - 安全情境的创建
  - 安全情境的删除
  - 授权结果等

DEMO：安全审计

应用场景1的一种解决方案



应用场景2的一种解决方案

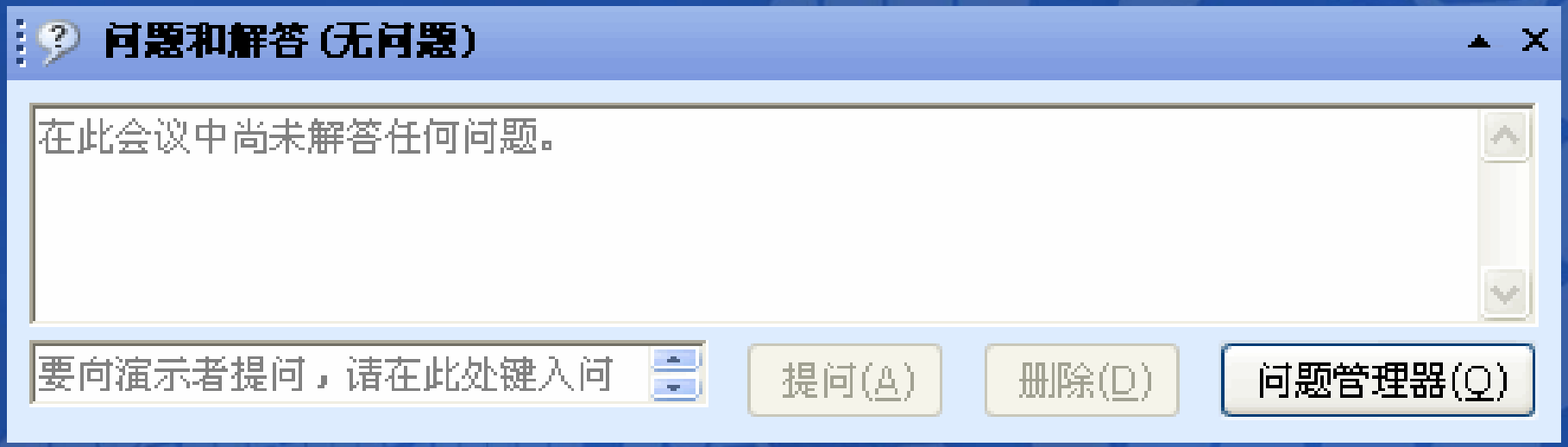


小 结

- **WCF**广泛支持**Web Service**系列安全规范
- 通常使用**Binding**进行配置
- **WCF**的通讯缺省即是安全的
- 支持多种凭证（**Credential**）类型
- **WCF**的安全架构具有很强的可扩展性

Question & Answer

如需提出问题，请单击“提问”按钮并在随后显示的浮动面板中输入问题内容。一旦完成问题输入后，请单击“提问”按钮。




您的潜力，我们的动力
Microsoft
微软（中国）有限公司
Microsoft
msdn
MSDN Webcasts