

Web Services Enhancements Beyond the Samples

Sven Aelterman
Principal Consultant

WSE 2.0

- Implement several WS-* specifications
 - **WS-Security***
 - **WS-SecureConversation***
 - **WS-Policy***, WS-SecurityPolicy
 - WS-Routing
 - WS-Addressing
 - WS-Trust
 - ...

* Will be covered in this session

ASMX vs. WSE

- Limited to IIS (in 2.0)
- Hosted in any application (demo 0)

WSE 2.0 vs. WSE 3.0

- .NET Fx 1.1
- Microsoft.Web.Services2
- ASMX only with IIS
- .NET Fx 2.0
- Microsoft.Web.Services3
- ASMX w/out IIS

Issues to be Aware Of

- WSE is supported
 - 2.0 has same support life-cycle as .NET 1.1
 - 1.0 support has ended
- WSE 1.0: Move to 2.0 ASAP
- Using WSE
 - Requires System.Xml
 - Requires System.Web
 - May require System.Web.Services

Demo 0: Web Services without ASMX

How to create web services using
WSE 2.0 without using ASMX

Web Service without ASMX

- Client-side proxy inherits from **SoapSender** or **SoapClient**
- Server-side service interface inherits from **SoapReceiver** or **SoapService**
- **SoapClient** and **SoapService** enable Request/Response paradigm
- Why? Think peer-to-peer...

Demo 0b: Re-use Service Interface

Re-use the service interface for SOAP over TCP in an HTTP scenario

Demo 1: Callback

Allow the server to call the client back with progress information

Callback Alternatives

- WS-Eventing (Microsoft, BEA)
- WS-Notification (IBM)
- Publish-and-Subscribe is a different paradigm

Caution: DoS attacks!!!

Secure Conversation

- To allow for less overhead in “conversations”
 - Long-running interactions between same client and server
- Encrypting and signing are expensive operations
 - Especially with asymmetric algorithms (X.509)
- Secure conversation uses symmetric **session** keys, exchanged using asymmetric encryption

Demo 2: Custom SCT

Create a secure conversation by
mimicking SSL

Improving the Custom SCT Solution

- Use multiple keys for session
 - Separate keys for
 - Signing by client
 - Encryption by client
 - Signing by server
 - Encryption by server
- Obtain server's public key through different channel than HTTP
 - Avoids "man-in-the-middle" attack

WS-SecureConversation with X.509

- Using X.509 allows use of Policy to verify signature
 - Man-in-the-middle attack: message intercepted, altered, and signed by attacker
 - Policy: allows service to specify which X.509 certs are acceptable
 - Before reaching service code (WSE pipeline)
 - Custom solution: identity needs to be checked in web method
 - May have to be done using X.509 also...

Issues with Exception Handling

- Default mechanism only returns SoapException
- Cannot serialize Exception classes to XML
- Security:
Can client be allowed to see exception details?

Demo 3: Exception Handling

Propagating Custom Exceptions
and Exception Information to the
Client

Related Resources

- WSE home
<http://msdn.microsoft.com/webservices/webservices/building/wse/default.aspx>
- New in WSE 3.0
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwse/html/newwse3.asp>
- Presentation & Code Download
<http://www.adduxis.com>

What's in the Download

- All code shown here
 - VS.NET 2003 and WSE 2.0 SP 3
 - VS 2005 RC0 and WSE 3.0 October CTP

Q&A

Sven Aelterman

sven@adduxis.com

<http://www.adduxis.com/blogs/blogs/sven>