使用 Web Services Enhancements 开发安全强大的Web Services

杨滔
v-tyang@microsoft.com
软件开发架构师
合作与开发技术部
微软（中国）有限公司

内容

- 回顾
- Web Services Architecture
- Web Services Enhancements (WSE) 2.0
- Demo

Connected Systems 回顾

- 实现设备、系统、人员和信息之间的无缝连接，体现应用软件的最大价值
- SOA为构建互联系统提供了架构指南
- Web Service是实现互联系统的重要技术
- 目前，基本的Web Service还无法满足企业级应用的要求

问题

- 如何开发安全的Web Service?
- 如何开发可靠的Web Service?
- 如何开发支持事务的Web Service?
- 如何在SOAP消息中传递非XML数据?
- ……

解决方案

- 开发自己的解决方案
  - 投入
  - 可重用性
  - 跨平台性和互操作性
- 使用的现成的解决方案
  - **Web Services Enhancements (WSE)** ✓

内容

- 回顾
- Web Services Architecture
- Web Services Enhancements (WSE) 2.0
- Demo

Web Services Architecture

目的

- 基于基本的 Web service
- 满足企业级应用的需求
  - Secure, reliable and transacted Web services
- 保留Web Service得以成功的优点
  - Interoperability
  - Ability to be implemented
  - Add no more complexity than needed

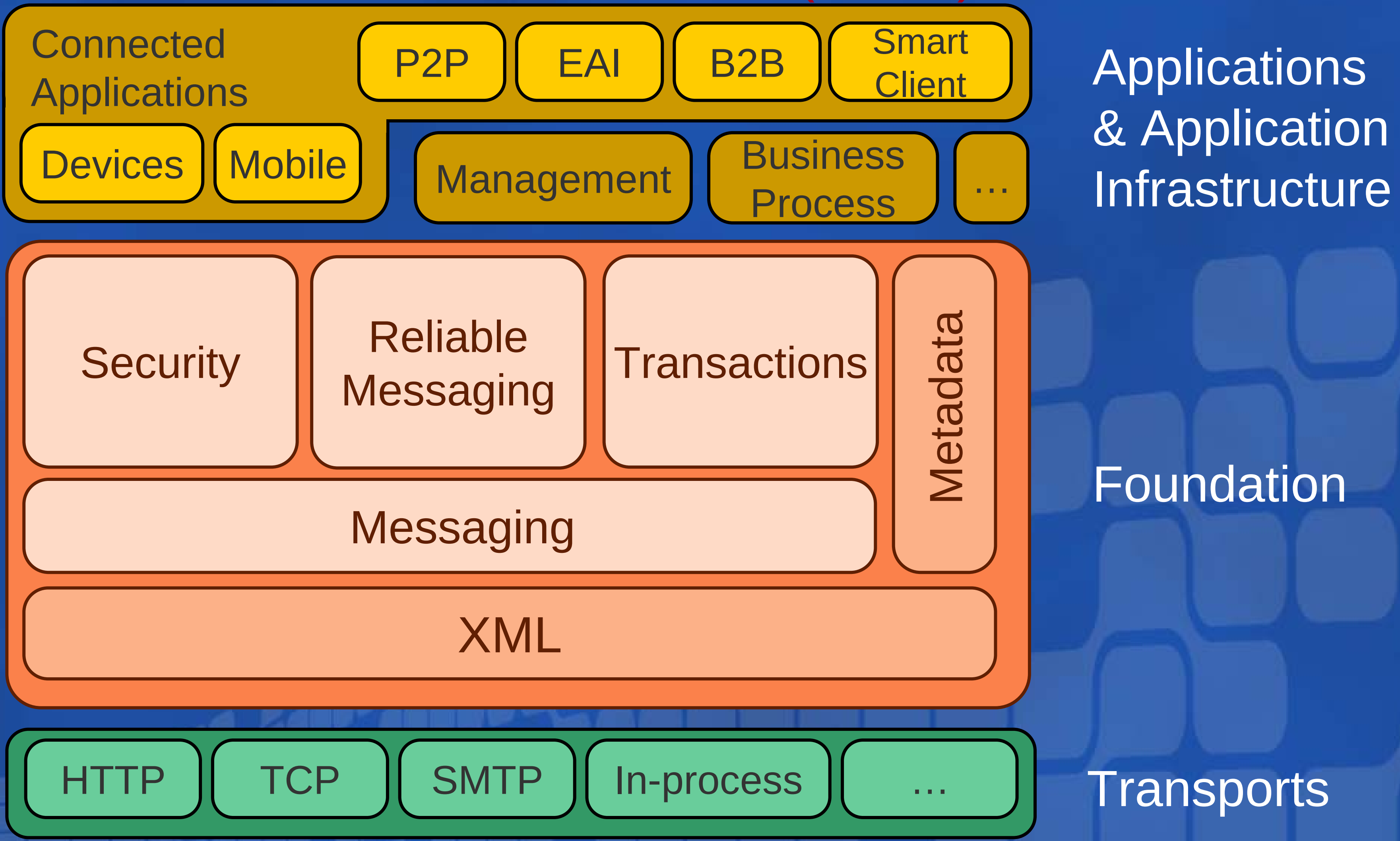
Web Services Architecture

Specifications

- Open standards process
  - Specification proposed by industry leaders
    - Microsoft, IBM, BEA, et al.
  - Initial implementations of proposed specifications
  - Feedback and interoperability workshops
  - Proposed specification submitted to standards bodies
    - W3C, IETF, OASIS
- WS-I promotes interoperability
  - Profiles interoperable use of specifications

Web Services Architecture

Web Services Architecture (WSA)



Connected Applications

P2P

EAI

B2B

Smart Client

Devices

Mobile

Management

Business Process

…

Applications & Application Infrastructure

Security

Reliable Messaging

Transactions

Metadata

Messaging

XML

Foundation

HTTP

TCP

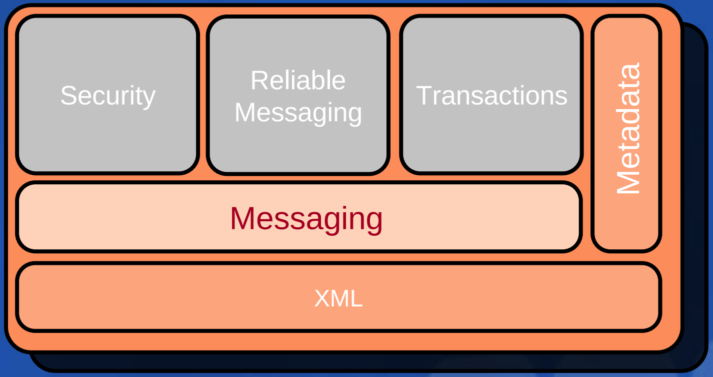
SMTP

In-process

…

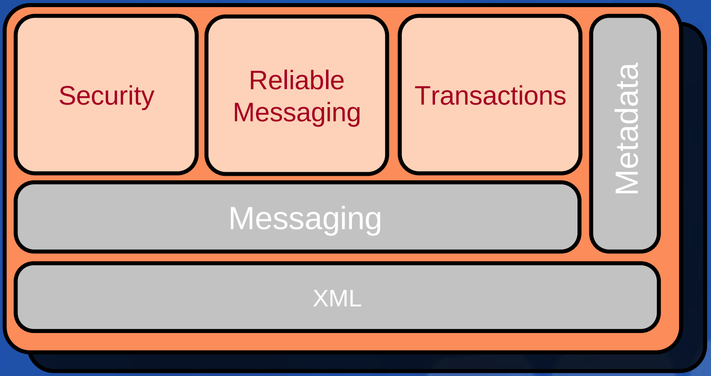
Transports

Web Services Architecture Overview – i



- XML
  - Interoperable data format
- Messaging
  - SOAP is the language of messages
  - Addressing enables general patterns of message exchange
  - Attach non-XML data to SOAP message
- Metadata
  - Discover services
  - Describe service interface with WSDL and XSD
  - Describe operational requirements with policy

Web Services Architecture Overview – ii



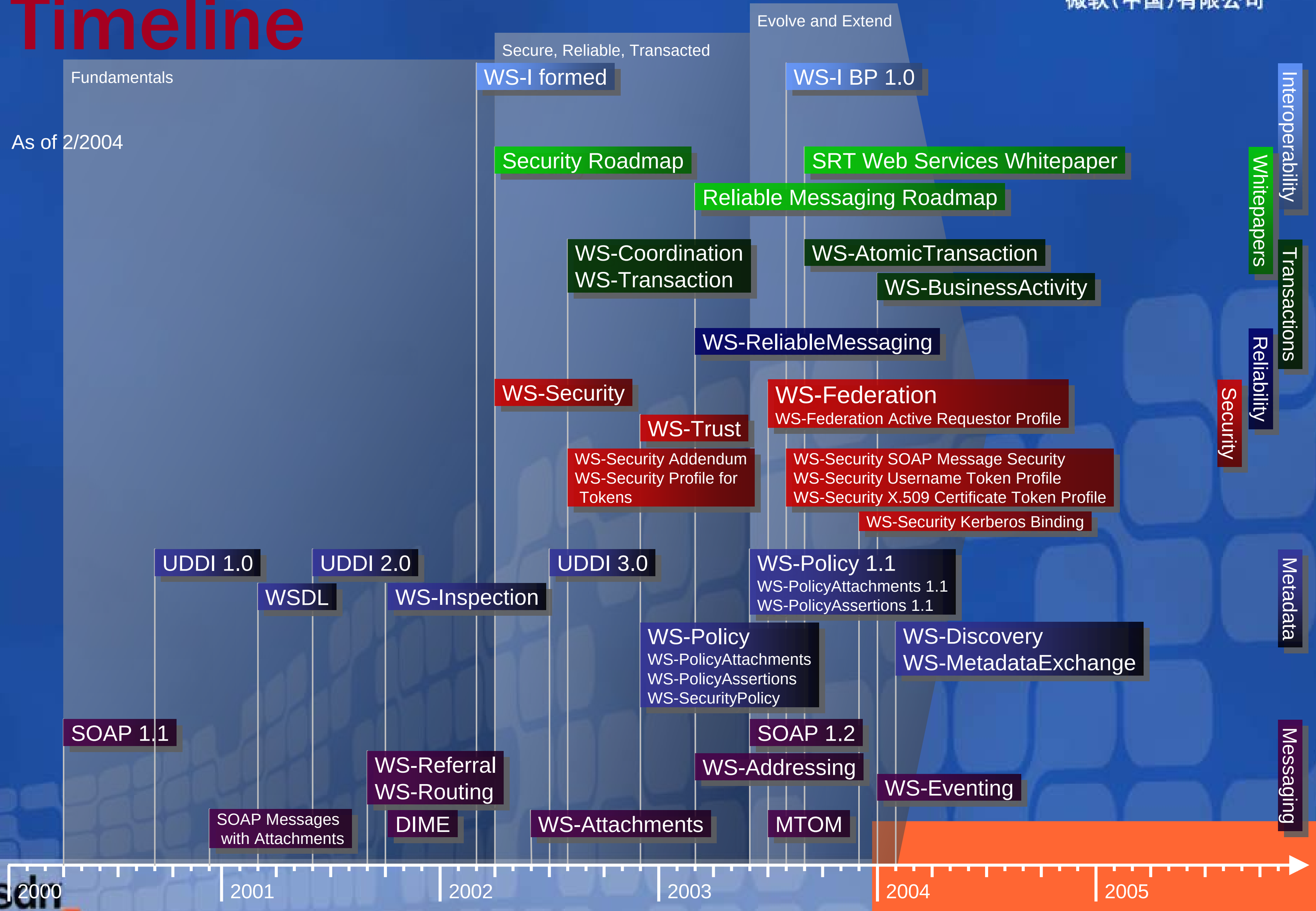
- Security
  - Critical for cross-organizational Web services
  - Authentication, message integrity, confidentiality, trust and privacy
  - Federation of security between organizations
- Reliability
  - Essential for mission critical applications
  - Ensure messages delivered and processed in order
- Transactions
  - Protect investment in transaction infrastructure
  - Extend to various kinds of distributed activities

Web Services Architecture Timeline

您的潜力，我们的动力

Microsoft 微软(中国)有限公司

As of 2/2004



Fundamentals

Secure, Reliable, Transacted

Evolve and Extend

WS-I formed

WS-I BP 1.0

Security Roadmap

SRT Web Services Whitepaper

Reliable Messaging Roadmap

WS-Coordination
WS-Transaction

WS-AtomicTransaction

WS-BusinessActivity

WS-ReliableMessaging

WS-Security

WS-Federation
WS-Federation Active Requestor Profile

WS-Trust

WS-Security Addendum
WS-Security Profile for Tokens

WS-Security SOAP Message Security
WS-Security Username Token Profile
WS-Security X.509 Certificate Token Profile

WS-Security Kerberos Binding

UDDI 1.0

UDDI 2.0

UDDI 3.0

WS-Policy 1.1
WS-PolicyAttachments 1.1
WS-PolicyAssertions 1.1

WSDL

WS-Inspection

WS-Policy
WS-PolicyAttachments
WS-PolicyAssertions
WS-SecurityPolicy

WS-Discovery
WS-MetadataExchange

SOAP 1.1

SOAP 1.2

WS-Referral
WS-Routing

WS-Addressing

WS-Eventing

SOAP Messages with Attachments

DIME

WS-Attachments

MTOM

Interoperability

Whitepapers

Transactions

Reliability

Security

Metadata

Messaging

2000

2001

2002

2003

2004

2005

msdn

内容

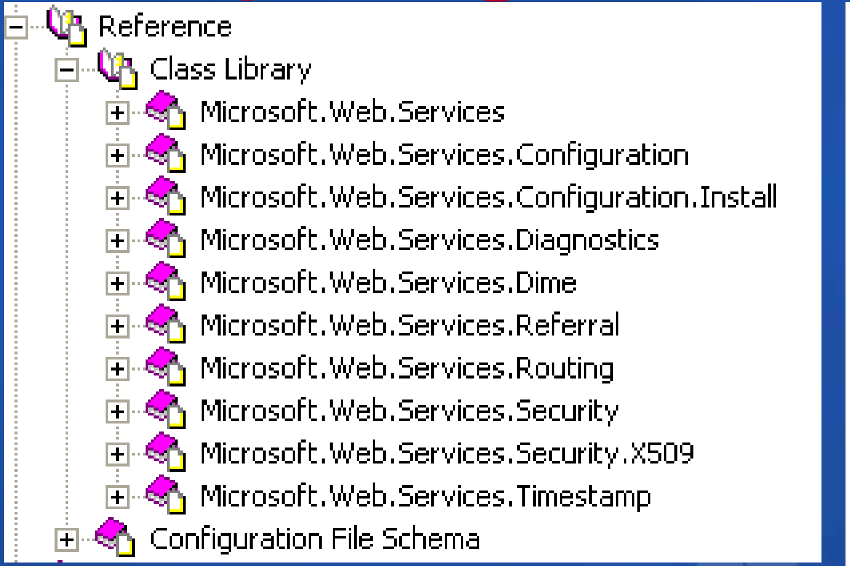
- 回顾
- Web Services Architecture
- Web Services Enhancements (WSE) 2.0
- Demo

WSE 2.0

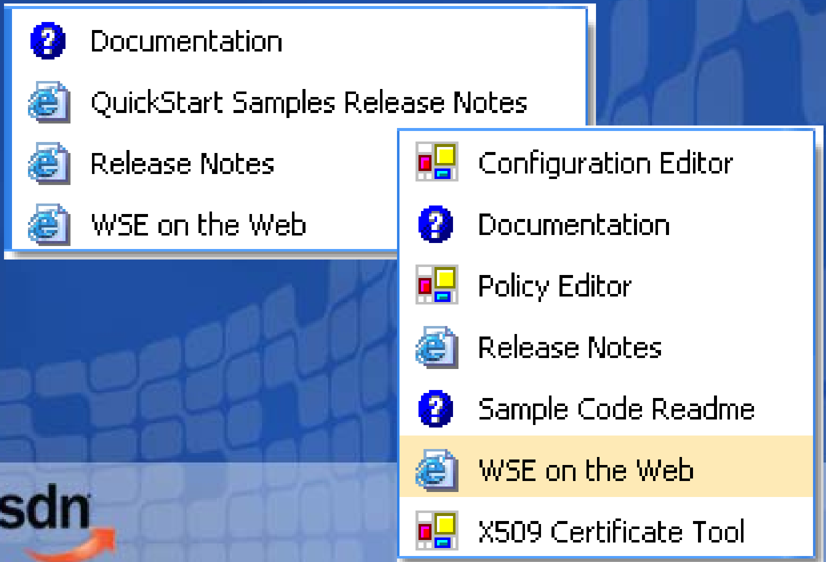
- 实施WSA提出的规范
- Visual Studio .NET Add-in
- .NET Framework 类库扩展
- 基于ASP.NET XML Web Services (ASMX)
- 版本发布的时间表与其他平台和工具的版本独立
- Microsoft对每个版本提供强有力的支持
  - 2 + 1 计划
    - 2年的主流支持计划
    - 1年的扩展支持计划

WSE 2.0

Comparing WSE 1.0 and 2.0

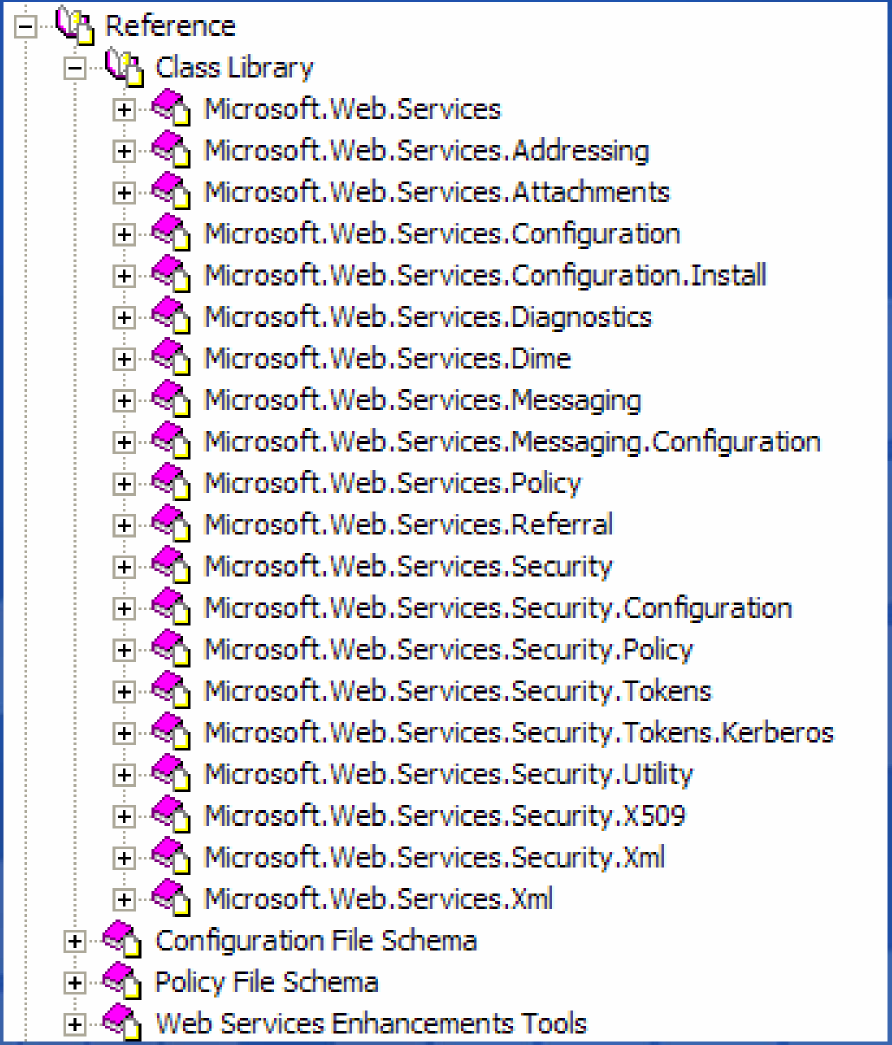


- Reference
  - Class Library
    - Microsoft.Web.Services
    - Microsoft.Web.Services.Configuration
    - Microsoft.Web.Services.Configuration.Install
    - Microsoft.Web.Services.Diagnostics
    - Microsoft.Web.Services.Dime
    - Microsoft.Web.Services.Referral
    - Microsoft.Web.Services.Routing
    - Microsoft.Web.Services.Security
    - Microsoft.Web.Services.Security.X509
    - Microsoft.Web.Services.Timestamp
  - Configuration File Schema



- Documentation
- QuickStart Samples Release Notes
- Release Notes
- WSE on the Web

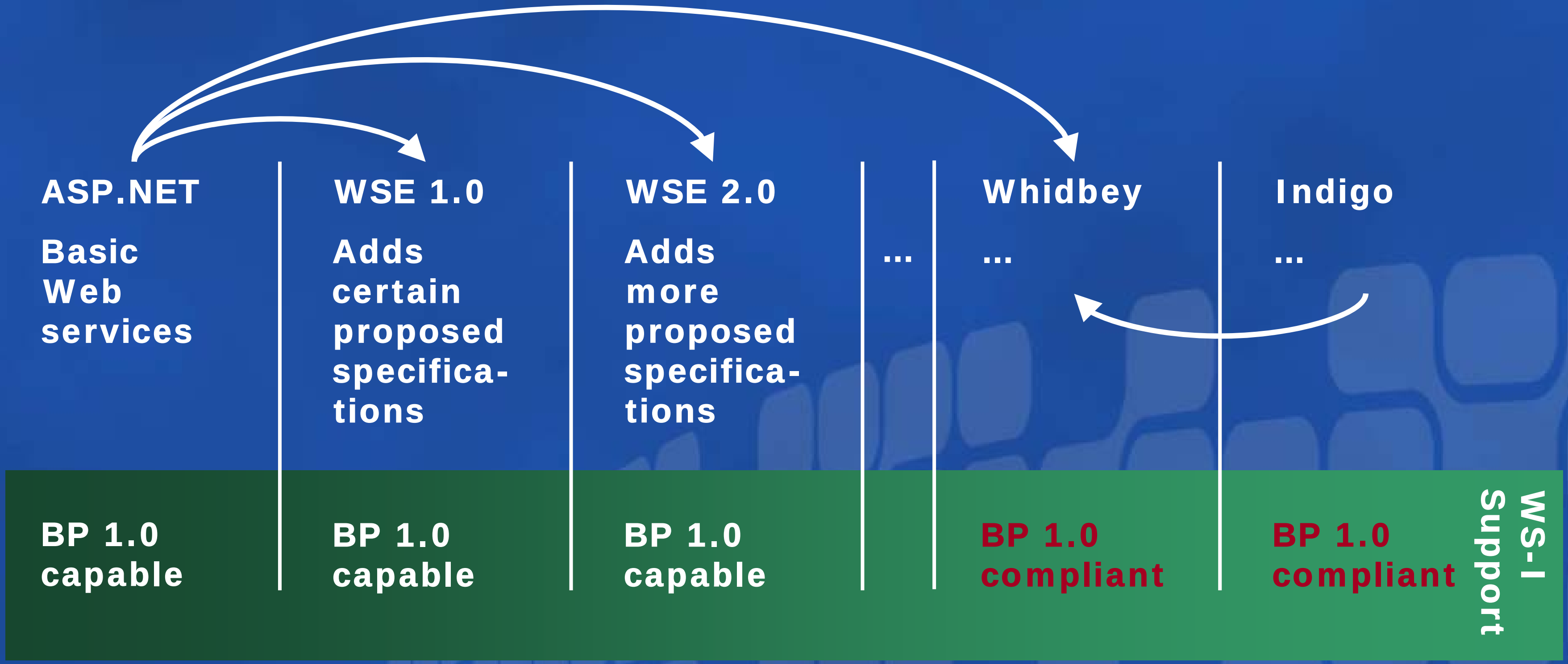
- Configuration Editor
- Documentation
- Policy Editor
- Release Notes
- Sample Code Readme
- WSE on the Web
- X509 Certificate Tool



- Reference
  - Class Library
    - Microsoft.Web.Services
    - Microsoft.Web.Services.Addressing
    - Microsoft.Web.Services.Attachments
    - Microsoft.Web.Services.Configuration
    - Microsoft.Web.Services.Configuration.Install
    - Microsoft.Web.Services.Diagnostics
    - Microsoft.Web.Services.Dime
    - Microsoft.Web.Services.Messaging
    - Microsoft.Web.Services.Messaging.Configuration
    - Microsoft.Web.Services.Policy
    - Microsoft.Web.Services.Referral
    - Microsoft.Web.Services.Security
    - Microsoft.Web.Services.Security.Configuration
    - Microsoft.Web.Services.Security.Policy
    - Microsoft.Web.Services.Security.Tokens
    - Microsoft.Web.Services.Security.Tokens.Kerberos
    - Microsoft.Web.Services.Security.Utility
    - Microsoft.Web.Services.Security.X509
    - Microsoft.Web.Services.Security.Xml
    - Microsoft.Web.Services.Xml
  - Configuration File Schema
  - Policy File Schema
  - Web Services Enhancements Tools

Web Services Enhancements

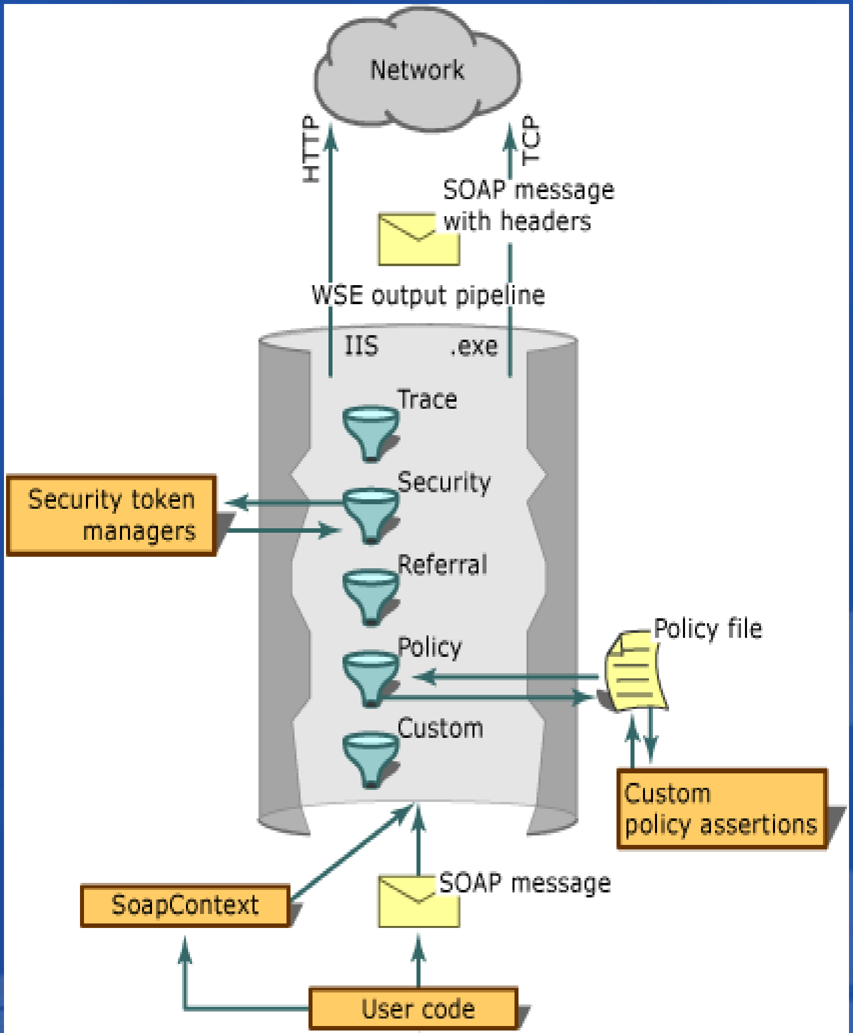
Roadmap

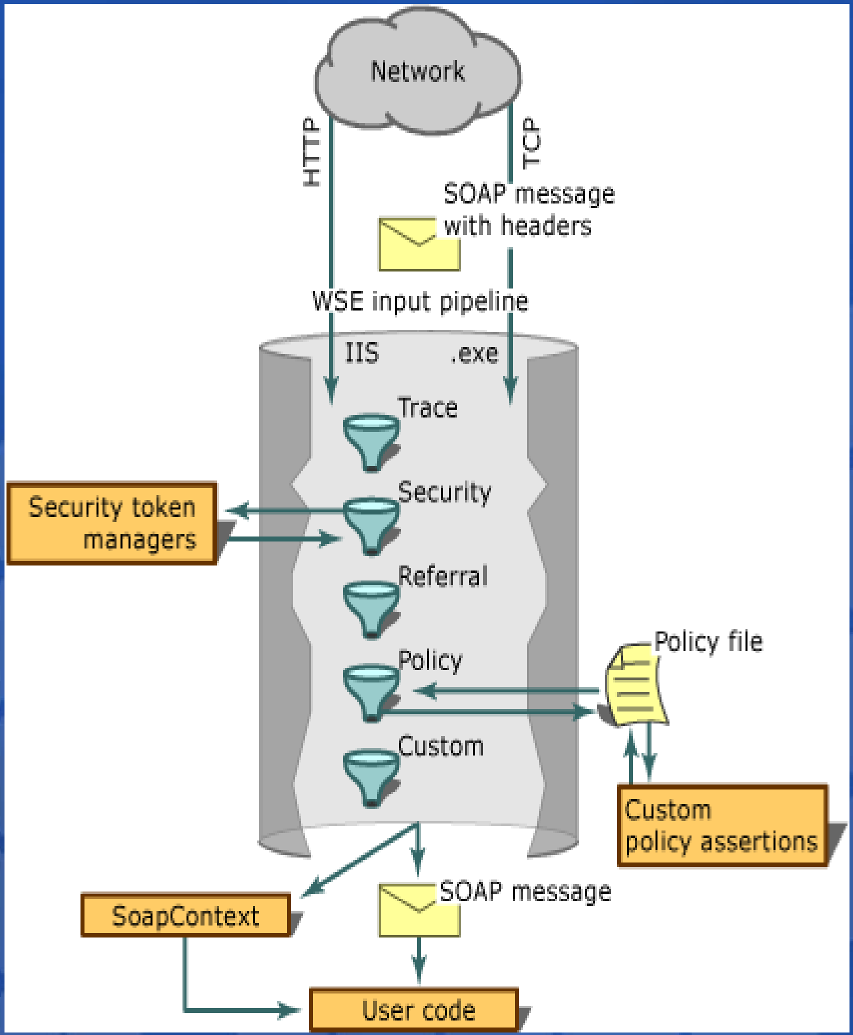


ASP.NET	WSE 1.0	WSE 2.0		Whidbey	Indigo
Basic Web services	Adds certain proposed specifications	Adds more proposed specifications	…	…	…
BP 1.0 capable	BP 1.0 capable	BP 1.0 capable		BP 1.0 compliant	BP 1.0 compliant

WS-I Support

WSE 2.0


Network
HTTP
TCP
SOAP message
with headers
WSE output pipeline
IIS
.exe
Trace
Security
Referral
Policy
Custom
Security token
managers
Policy file
Custom
policy assertions
SoapContext
SOAP message
User code


Network
HTTP
TCP
SOAP message
with headers
WSE input pipeline
IIS
.exe
Trace
Security
Referral
Policy
Custom
Security token
managers
Policy file
Custom
policy assertions
SoapContext
SOAP message
User code

WSE 2.0

Security of Critical Importance for Web Services

- Organizational requirements
  - Regulatory conformance
  - Privacy
  - National security
- Vulnerability points
  - Network
  - Operating system
  - Web server (IIS)
  - ASP.NET platform

WSE 2.0

Security

- Authentication
  - Support for common types
- Integrity
  - Nonrepudiation: verify the sender
  - Verify message contents
- Confidentiality
  - Privacy
  - Symmetric and asymmetric cryptography

Traditional Security Options

Introduction

- Secure platform and transport
  - Best for corporate intranets
  - IIS + ASP.NET
  - SSL or IPSec
- Securing the Web service
  - Messages travel end-to-end, not point-to-point
  - The message itself has to be secured
- Implement custom code
  - Difficult to write and test
  - Maintenance
  - Non-.NET client support

Standards-Based Security

Web Services Enhancements 2.0 (WSE)

- Authentication
  - Integration with Windows security structure via the Principal object
- Authorization
  - IsInRole checks for group membership
  - Centralized management of security
- Digital Signature
  - Integrity check
  - Non-repudiation
- Encryption

Standards-Based Security

WSE Token Support

- WSE supports the following tokens:
  - Username
  - Kerberos
  - X509
  - Security Context
  - Custom XML token
- Not all tokens are equal
- Tight integration with Windows security infrastructure (Principal)
- Custom authentication

WSE 2.0
Secure Conversation

- Issue security context tokens for a conversation
  - Uses symmetric key for conversation
  - Fewer computational resources required to sign and encrypt than with asymmetric keys
- Change from WSE 1.0

Policy

Separating Operational & Functional Requirements

- Policy governs the operational requirements of a Web service
  - Functional requirements addressed during development
  - Operational requirements addressed in deployment and maintenance
    - These change over time and location
- Defined in the WSA specifications
  - WS-Policy
  - WS-PolicyAssertions
  - WS-PolicyAttachments
  - WS-SecurityPolicy

WSE 2.0
Messaging and Transports

- Transports
  - Support for HTTP, TCP, in-process
- Messaging
  - WS-Attachments and DIME
    - Payload appended after SOAP envelope
    - Will be superseded by MTOM
  - WS-Addressing

WSE 2.0
Attachments

- Data that is hard to serialize
  - Binary data
  - Encoded data
  - Large XML documents
- DIME
  - Payload appended after SOAP envelope
  - SOAP envelope availability
  - WS-Attachements and DIME will be superseded by MTOM
    - Addresses concerns such as securing attachments

Demo

- Attachment
- TCP
- Security
- Policy

Summary

- What you learned
  - WSA defined by proposed open specifications
  - WSE implements proposed specifications
  - WSE 2.0 provides rich functionality
- Next steps
  - Examine your current architecture
  - Examine current and future needs
  - Could you benefit from WSA?
  - Web Services Developer Center on MSDN

Resources

- MSDN中文网站
  - http://www.microsoft.com/china/msdn/
- Web Services Developer Center
  - http://msdn.microsoft.com/webservices/

您的潜力，我们的动力

Microsoft®

微软（中国）有限公司

Microsoft®