

# Securing Java Web Services (2 Days)

**Custom Training Institute**  
9085 Coyote Springs Road  
Prescott Valley, AZ 86314  
(928) 772-3811  
FAX (928) 441-6444

## Securing Java Web Services (CTI 562)

*This course introduces Java developers to key technology for developing secure Web services: XML signature and encryption standards, the Java APIs to support them; the Security Assertions Markup Language (SAML) and eXtensible Access Control Markup Language (XACML).*

Prerequisites: Experience developing Java Web services is assumed - either via SAAJ or JAX-RPC. Students are expected to be able to read and write XML fluently, and have some familiarity with XML Schema.

Minimum software requirements: Microsoft Windows or Linux systems that support J2EE 1.4. A mix of free downloadable tools will be specified for setup.

Minimum hardware requirements for all machines: Pentium 2+GHz or equivalent CPU, 512 meg RAM, 1 gig HD space.

Microsoft PowerPoint and Internet access on instructor's workstation for presentation purposes.

### Module 1: Web-Service Security

- Web Services and Security
- Threats
- Technology and Techniques
- J2EE Techniques
- Securing Web-Service URIs
- HTTPS
- Interoperable Security
- Technology Stacks: WS-Federation and Liberty Alliance
- Securing XML Content
- W3C Standards: XML Signature, Encryption and Canonicalization
- The Single Sign-On Problem
- OASIS Standards: SAML, XACML, and WS-Security

### Module 2: XML Security Standards

- The W3C
- XML Digital Signature
- Canonical XML
- Enveloped, Enveloping, and Detached Signature
- XML Encryption
- Configuring Signature and Encryption for JAX-RPC Services

### Module 3: Java APIs for XML Security

- The Java Cryptography Extensions
- The Java API for XML Digital Signature
- Signing XML Nodes and Trees
- Verifying Signatures
- The Java API for XML Encryption
- Encrypting XML Content
- Integrating Cryptography into SAAJ Services and Components

### Module 4: The Security Assertions Markup Language

- History of SAML
- Goals and Non-Goals
- Authorities
- Assertions
- Protocol

### Module 5: SAML Assertions

- The Assertions Schema
- Extensibility
- Assertions and Subjects
- NameIdentifiers and SubjectConfirmations
- AuthenticationStatements
- AttributeStatements
- AuthorizationDecisionStatements
- Actions and Evidence

### Module 6: SAML Protocol

- SAML Messaging
- The SAML Protocol Schema
- Request Types
- Response Types
- Status and StatusCode
- AuthenticationQuery
- AttributeQuery
- AuthorizationDecisionQuery
- Signing SAML Assertions and Messages
- WS-Security and SAML Tokens

### Module 7: The eXtensible Access Control Markup Language

- Interoperable Policy Statements
- XACML
- Subjects, Actions, and Resources
- Policies and PolicySets
- Targets and Rules
- Overlaps with SAML

### Appendix A: Learning Resources

### Appendix B: XML Namespaces for Security Standards