Training: Capstone Courseware
562 Securing Java Web Services

TRAINING GOALS:

This advanced course introduces Java developers to key concepts and technology for developing secure web services and securing enterprise software architecture. Though consensus is forming, and standards have largely taken shape, this is still a broad and challenging field. We focus on a few well-defined approaches: XML cryptography, the WS-Security and WS-SecurityPolicy standards, and the Security Assertions Markup Language, or SAML. We also look XACML for authorization policies, and at trust and federation -- not only as envisioned by SAML but also through the WS-Trust and WS-Federation specifications.

These approaches do overlap, and through our primary case studies we present a single, coherent story of assuring confidentiality, integrity and non-repudiation, user authenticity, and proper request authorization with a blend of policy-driven WS-Security, SAML, and even some application-coded digital signature. We also investigate the web-application end of SAML, with an in-depth study of single sign-on and federated identity.

Although for practical purposes this course relies on a specific platform, which is Java EE, the great majority of the course content teaches interoperable specifications, and would be equally useful to developers working on other web-service-capable platforms such as .NET -- or to those who work with multiple platforms, and do need to understand the interoperable pieces in detail but perhaps don't need to delve into implementation strategies. In fact, customizations are available that essentially leave out the Java to stick more strictly to the XML.

CONSPECT:

- Chapter 1. Securing the Service-Oriented Enterprise
  - Security for Web Services
  - Threats
  - CIA Goals
  - Solution Levels: W3C, OASIS, Java EE
  - Scenario: Secure Multi-Party Conversation
  - Cryptography
  - WS-Security and WS-SecurityPolicy
  - Scenario: Sharing Security Information
  - SAML and XACML
  - Scenario: Multiple User Realms

Appendix B. Web-Service Security Prefixes and Namespaces

REQUIREMENTS:

- Solid **Java programming** experience is essential - Course 103 provides excellent preparation.
- Experience **developing Java Web services** is likewise a hard requirement: labs will assume understanding of both SAAJ and JAX-WS - Course 561 is strongly recommended.
- Students are expected to be able to read and write **XML** fluently, and have some familiarity with **XML Schema**. Consider courses 501 and 517.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Capstone Courseware.

TRAINER:

Authorized Capstone Courseware Trainer.