Eclipse Summit Europe 2007

ALF Releases Authentication and Identity for Development Tool Integration

Brian Carroll
Eclipse ALF Project Lead
bcarroll@serena.com
Outline

- Brief Intro to Eclipse ALF
- The Problem
  - Conveying Identity among integrated tools
- The Solution
  - SSO, SAML, Higgins, and WS-*
- Next Steps
A Brief Introduction to Eclipse ALF
ALF: Is About Process Integration
Dream: What the customer thinks they bought
Nightmare: What the customer is implementing

Business Visualization

Requirements Management

Provisioning

Performance Monitoring

Deployment

Release Management

Test Management

Build Management

Change Management

Issue Management

Portfolio Management

Project Management

Resource Planning

Modeling

prototyping
Time to wake up: What the customer wants
Introducing the Application Lifecycle Framework (ALF)

- A common platform for tool integration
- SOA-based runtime
- Eclipsed-based tool
- Support for heterogeneous platforms
- Vendor neutral
- Standards based
- Extensible

Application Lifecycle Framework

- Event Manager
- Service Orchestration (Pluggable BPEL Engine)
- Administration (Eclipse Plug-in)
- Identity and SSO

Vocabularies & Best Practices

ALM Tool A
ALM Tool B
ALM Tool C
ALM Tool D

WS Intf
WS Intf
WS Intf
WS Intf
ALF High-level Architecture

**ALF Design Time**
- **Vocabularies, Best Practices**
- Administration (Eclipse Plug-in)
  - Events
  - Services
  - ServiceFlow
- Pluggable BPEL Designer

**ALF Runtime**
- Identity and SSO tool wrapper (ALF Gateway)
- Event Manager
- Service Orchestration (Pluggable BPEL Engine)
- STS (Higgins, …)
- Authentication Authority (e.g., LDAP)
- Common Services

Metadata about a tool’s SOA interfaces

ALF-enabled Tools
ALF: Is About Process Integration

ALF Event Manager

Event 1
  Action 1
  Action ...
  Action n

ALF Service Flows

Inception
Definition
Construction
Verification
Implementation
The Problem: 
Conveying Identity among 
Integrated Tools
ALF: Is About Process Integration
The Solution:
SSO, SAML, Higgins, and WS-*
Trends in Security

- “Factoring out” authentication from the application
  - Avoids having your critical security logic written by “Joe Developer”
  - In production, you can focus more infrastructure hardening efforts on just a handful of security components
- Make it easier for tools and applications to implement security
- Adoption of SAML Assertion as a token format
ALF Single Sign On

- ALF has two related mechanisms:
  - A means for a user at a tool to obtain a standardized SAML token that proves he has authenticated (i.e., SSO)
    - Similar to obtaining a drivers license at the DMV
    - Token life is typically set to approximate a workday
  - A means for conveying that standardized token through Events and the tools that are invoked by the resulting BPEL Orchestration
    - But Orchestrations may run for longer that a workday
    - So a variant with longer life that is bound to the service flow is used
The Web Services Security Stack

**WS-Security**
- WS-SecureConversation
- WS-Federation
- WS-Authorization
- WS-SecurityPolicy
- WS-Trust
- WS-Privacy
- Kerberos Profile
- x.509 Profile
- Username Profile
- SAML Profile

**Underlying WS Specs**
- WS-Policy
- WS-Addressing
- WS-Utility

**Underlying XML Specs**
- XML Encryption
- XML Canonicalization
- XML Digital Signature

**Existing (established) Security**
- PKI / x.509
- Encryption Algorithms
- Kerberos
- Hash and Digest Algorithms

**Recent Security**
- SAML

Eclipse ALF Project  http://www.eclipse.org/ALF
Key Standards used

- Both ALF and Higgins use
  - WS-Security
    - Username Token
    - SAML Token
  - WS-Trust
  - WS-Federation
    - Passive Requestor Profile (Web application)
  - SAML Assertion 1.1
  - XML Canonicalization and Digital Signature

- Higgins also uses
  - LDAP
The ALF WSS Implementation Stack

WS-Security
- WS-SecureConversation
- WS-Security Policy (Apache Rampart)
- WS-Federation (Eclipse ALF SSO Gateway, Eclipse Higgins STS)
- WS-Trust (Eclipse ALF SSO Common, Eclipse Higgins STS)
- WS-Federation (Eclipse ALF SSO Gateway, Eclipse Higgins STS)
- WS-Trust (Eclipse ALF SSO Common, Eclipse Higgins STS)

WS Security Framework (Apache Axis2)
- Kerberos Profile
- Username Profile
- x.509 Profile
- SAML Profile (OpenSAML)

Underlying WS Specs
- WS-Policy (Apache Neethi)
- SOAP (Axis2)
- WSDL (Woodstox)
- WS-Addressing (Axis2 Rampart)
- WS-Utility (Axis2 rampart)

Underlying XML Specs
- XML Encryption (Apache WSS4J)
- XML Digital Signature (Apache WSS4J)
- XML Canonicalization (Apache WSS4J)

Existing (established) Security
- PKI / x.509
- Encryption Algorithms
- Kerberos
- Hash and Digest Algorithms

Recent Security
- SAML (Internet2 Shibboleth OpenSAML)
Gatekeeper – “Invisible protective shield” – Making it easy

Unwanted germs

Web–based tool

ALF Gatekeeper

Messages without proper user credentials
Sample SSO components and flow
ALF Orchestration Identity Passing

- ALF Gatekeeper
- Tool A
- ALF Event Manager
- ALF ServiceFlow
- BPEL Orchestration Engine
- Tool B
- Tool C
- Higgins Identity Project
- STS (Token Server)
- LDAP Directory
- User
- ALF Logon App (Servlet)
Conclusion
Status and Next Steps
Current ALF status

- Uptake of ALF by first commercial tool
  - Serena Mashup Suite

- Milestone 0.8
  - Source code is available now in Eclipse CVS
    - Includes all the SSO and Identity code
  - Eclipse IP review of 3rd party dependencies in progress
  - Release Review in November
Next steps

- Ongoing support for commercial tools
- Evangelism and community building
  - Now that we have the framework, …
  - Show it off with demos
- Security extensions
  - Expand security token types supported
    - Kerberos Tickets and X.509 Certificates
  - Expand platforms to desktop and Eclipse IDE
    - Equinox JAAS
  - Interoperability with other commercial and custom authentication mechanisms via WS-Federation
- Major goal is ALF 1.0 – Out of incubation
Questions?

Get Involved!

Catch me at during the Summit for a demo!

Thank you!