ALF SSO: Security Framework for Tool Integration

Brian Carroll, Eclipse ALF Project Lead
bcarroll@serena.com
ALF: Is About Process Integration
What is ALF SSO

- Once we had the Event and BPEL Orchestration working, we needed to know who was responsible for initiating all the activity performed in an Orchestration
  - Tools tend to have authorization mechanisms to control who can perform what operations on what data

- Web service standards provide the mechanism for conveying an identity
  - WS-Security defines a standard way to convey an identity through web service calls
  - SAML defines a standard token format
  - *But where do we get the identity in the first place?*
Sample SSO components and flow: Obtaining an SSO token

Higgins Identity Project

ALF Logon App (Servlet)

STS (Token Server)

Id Attr Server

Context Provider

LDAP Directory

User admin

User

ALF Gatekeeper

Tool A

Tool B

ALF Gatekeeper
ALF Orchestration Identity Passing

Tool A → ALF Event Manager → Tool B
Tool A → ALF Gatekeeper → Tool C
User → ALF Logon App (Servlet) → Higgins Identity Project

ALF ServiceFlow
BPEL Orchestration Engine
STS (Token Server)
LDAP Directory
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

• And, more of a reality than a trend:
  - Things in security change slowly
    - E.g., Still have to support legacy authentication schemes
Gatekeeper – “Invisible protective shield”

Unwanted germs

Web-based tool

ALF Gatekeeper

Messages without proper user credentials
Key Standards used

• ALF leverages components from the Eclipse Higgins (Identity) project
• 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
  - LDAP to access Authentication Authorities
So why consider ALF Security?

• ALF SSO provides a standards-based way to:
  ▷ Factor-out tricky security logic from application (tool) programming
    ▪ ALF Gateway
  ▷ Based on standards:
    ▪ SAML tokens
    ▪ WS-Security family
  ▷ Conveys identity across web services integrations

• Saves you from reading and implementing thousands of pages of WS-* and Security specifications
  ▷ Implementation has been tested
    ▪ Consumed by a commercial product: Serena Business Mashups
What’s Next?

• Expand beyond web applications to desktop tools
• To interoperate with other credentials formats and approaches
  ▪ X.509 (as found on SmartCards)
  ▪ Kerberos Tickets (e.g. Windows logon Security)
  ▪ Microsoft CardSpace
• To federate with existing authentication schemes
Thank you!

Check it out and get involved!

www.eclipse.org/alf