SOA: Protecting the Architecture by Leveraging Standards

Suneet Shah
Diamelle Technologies
www.diamelle.com
suneet@diamelle.com
Agenda

- Current Business Challenges
- SOA Implementation Challenges
- Summary of Current Standards
- Solution
- Considerations for Maturing and Globally Distributed SOA
- Future Possibilities
Current Business Challenges

Extended Enterprise and Faster Time to Market
- Support business processes across company boundaries
- Globalization creates new business opportunities across boundaries
- Globalization also creates a more competitive environment

Improve Operational Efficiencies
- Need to lower IT costs and operational overhead
- Duplication of business logic and data creates high development, maintenance and administration costs

Governance and Compliance
- Conformance to policy and audit-ability
- Privacy
- Protection against internal and external attacks
Addressing Challenges with SOA

- SOA addresses business challenges
- Unlike past industry attempts, there is a high level of consensus among vendors and end-user corporations
- Results in accepted standards driven by organizations such as Liberty Alliance, OASIS and others.
- SOA does not come without its share of organization and technological challenges
- Following slides will explore these challenges from:
  - Security perspective
  - Available standards
  - Solutions
### Challenges Implementing SOA

- Rapid Adoption of SOA, but most web services standards looked at security as an after thought
  - Identity is not well integrated
  - Web services (HTTP) are protected,
  - Non-web services, ESB, etc are not protected
- Various SSO solutions cannot easily co-exists in heterogeneous environment
- Propagating SSO tokens / assertions across SOA
- How to enable fine grained authorization or data level entitlements
  - Traditional IDM solutions have been more focused on a coarse grained activities
- Point solutions exist for much of this.
  - Lose benefits of centralized administration or consistent definition and enforcement of policy
  - Start to create new silos of security information
- Most application architects and developers do not understand the role IDM plays in SOA
  - Applications with no clearly defined security infrastructures which isolate applications from the underlying security infrastructure
## Applicable Standards

<table>
<thead>
<tr>
<th>Complementary Standards</th>
<th>Liberty Identity Federation Framework (ID-FF) &amp; Security Assertion Markup Language (SAML) 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>eXtensible Access Control Markup Language (XACML 2)</strong></td>
<td>Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management</td>
</tr>
<tr>
<td>Provides a framework to define and enforce which users have access to specific resources</td>
<td></td>
</tr>
<tr>
<td><strong>Liberty Identity Web Services Framework (ID-WSF)</strong></td>
<td>Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles</td>
</tr>
<tr>
<td><strong>Liberty specifications build on existing standards (SAML, WS-Security)</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Complementary Standards**

- WS-Policy
- WS-Trust
- WS-Addressing
Creating the Solution

Solution needs to be able to do the following:

- Exist in heterogeneous environments where you need to support various formats of authentication tokens.
  - Even with standards we need to support SAML 1.0, SAML 1.1, SAML 2, ID-FF, etc
  - Each vendor has their own proprietary format that pre-dates federation work
  - Other tokens: Kerberos, X.509
- Enforce course and fine grained entitlements
- Enforce policies throughout SOA
- Apply the notion of network identity such that:
  - Consumers can maintain their privacy
  - Corporations and manage customer relationships without 3rd party involvement.
WS-Trust provides a framework through which one type of token from a trusted domain can be translated into its equivalent for a different format.
Enforcing Authorization policies

- XACML complements SAML to provide authorization framework
- Enable authorization at different levels of granularity
- Need enforcement points to apply rules
Identity Services

- Identity based services:
  - Services that are being invoked are specific to a particular identity or set of identities.
  - Service acts up on resources for a particular identity or set of identities.
  - Improved privacy through limited release of personal information

- ID-WSF 2 provides a framework for:
  - Discovering and invoking identity based services
  - Permission based attribute sharing which can be done under the users control or on their behalf
  - Notifications
  - Leverages SAML assertions to represent identity
  - Uses WS-Security for message level security

- Uses WS-Addressing to allow support for:
  - Asynchronous messages
  - Multi-path messaging which can be used in system to system communication
Identity Enabled SOA – Bringing it Together
Additional Considerations

- Globally distributed architectures
  - Local regulations and their impact on policies
  - Federated ESB’s
  - Service virtualization
- SOA Governance
As adoption of SOA matures, companies need a governance strategy

Runtime and Design time governance

Governance provides people with authority to supervise, monitor and control the direction of an entity

Common SOA Governance activities includes:

- Defining and monitoring SLA’s
- Service versioning strategies
- Identifying services candidates and subjecting them to committee review for approval
Governance activity outcomes impacting security:

- Security policies
- SLA
- Service versioning
  - Multiple versions of a service may co-exist
  - Each version may have variances in the security policy
  - Need to determine the impact on your authorization model
Future Possibilities
Federated Authorization

- Federated Authorization:
  - Allows you to factor out authorization and place it at a logical location
- Two use cases
  - SAML based Approach
    - User authenticates and receives SAML assertion with a set of attributes
    - User tries to access a service provider in a different domain
    - Service provider acts as both a policy decision point (PDP) and policy enforcement point (PEP).
    - Access control decision is made based on the attributes
  - SAML and XACML Based Approach
    - Policy decision point (PDP) and policy enforcement (PEP) are distributed
    - User authenticates and receives SAML assertion without attributes
    - User tries to access service provider in a different domain
    - Service provider call the PDP to evaluate the request based on policy
    - PEP will enforce the PDP’s request.
Identity Aware COTS

- ISVs engaging enterprise customers are increasingly SOA and security standards in the products
  - Ie. Oracle, SAP, Documentum, Salesforce.com
- Approach facilitates integration with enterprise infrastructure
- Facilitates enforcement of corporate policies
- Building on SOA with Identity enabled strives towards a plug and play nirvana
- Availability of cost effective tools and open source initiatives facilitates this goal
  - OpenIAM – Diamelle Technologies
  - OpenSSO, Etc.
Significant amount of work has gone into the evolution of SOA and Identity standards in the past few years.

While still evolving, they have matured to the point where they:

- Build upon each other and use common elements such as SAML
- Offer the ability to protect enterprise SOA initiatives for both internal and external facing system
- Capabilities are being realized by vendors on both the SOA and IDM side.

SOA and IDM complement each other.

- IDM standards make extensive use of SOA
- SOA needs IDM
Q & A
Thank You
References

- **Specifications:**

- **Others:**