SPML (Service Provisioning Markup Language) and the Importance of it within the Security Infrastructure Framework for eBusiness

Gavenraj Sodhi

Senior Technology Analyst

Provisioning Services Technical Committee, OASIS

June 2002

Orlando, Florida

Interoperability Summit 2002

Overview

Goal 1: Standardizing and simplifying the interoperability of systems requiring identity information from a multitude of systems and organizations

Goal 2: SPML, with other emerging standards, needs to interoperate and deliver a comprehensive interoperable standards-based infrastructure for eBusiness

Agenda

- What is the Problem?
- What are some standards that may play?
  - SPML Concepts
  - SAML Concept of Back Office Transactions
  - XACML Concept
  - XKMS Authentication Service
- Conceptual eBusiness Framework with Standards Stack
- Example of how eBusiness may use these standards
  - Business and Technological Case Representation
- Q&A

What is the problem?

- Currently a mess of standards which have been developed and are currently under development

- How do they fit in the standard's pyramid and how do fix the real problems you are trying to solve for your customers?

- The handling of the Identity has to be secure and properly handled across systems

Standards-based Components that are needed to solve the problem

Components that are needed for a smooth secure transaction to occur:

- A Standards framework that allows the exchange of authentication and authorization data between security systems of one or many organizations.
- A Standards framework that reuses existing authorization information/credentials to access backend resources and services of one or many organizations.
- A Standards framework that provides fine-grained access control to bill back the use of a resource and/or a service used by a system entity's division or organizational unit.
- Plug ability of a Certificate-based authority system to provide third-party authentication assertion to authenticate the system entity to access a resource and/or a service.
- Common definitions is very important to be consistent.

SPML Concepts

The PSTC (Provisioning Service Technical Committee) working group is developing SPML, which is a proposed specification that addresses the required semantics for Provisioning Service Points (organizations) to exchange data (I.e., Identity) requests relating to the managed Provisioning Service Targets (resource or service).

SPML may dictate the provisioning activity of Provisioning Service Points (PSP) and Provisioning Service Targets (PST) based on an Authorization Decision Assertion (I.e., SAML).

- Add/Create
- Delete
- Modify
- Query

SAML Concepts

SAML is a XML standard for exchanging authentication and authorization data between security systems.

The SAML Domain model and specifications permit Authentication and Identity information to be federated among multiple organizations and servers.

SAML provides the following:

- XML-based framework for exchanging security information
  - XML-encoded security “assertions”
  - XML-encoded request/response protocol

XACML Concepts

A few aspects of XACML (eXtensible Access Control Markup Language) are:

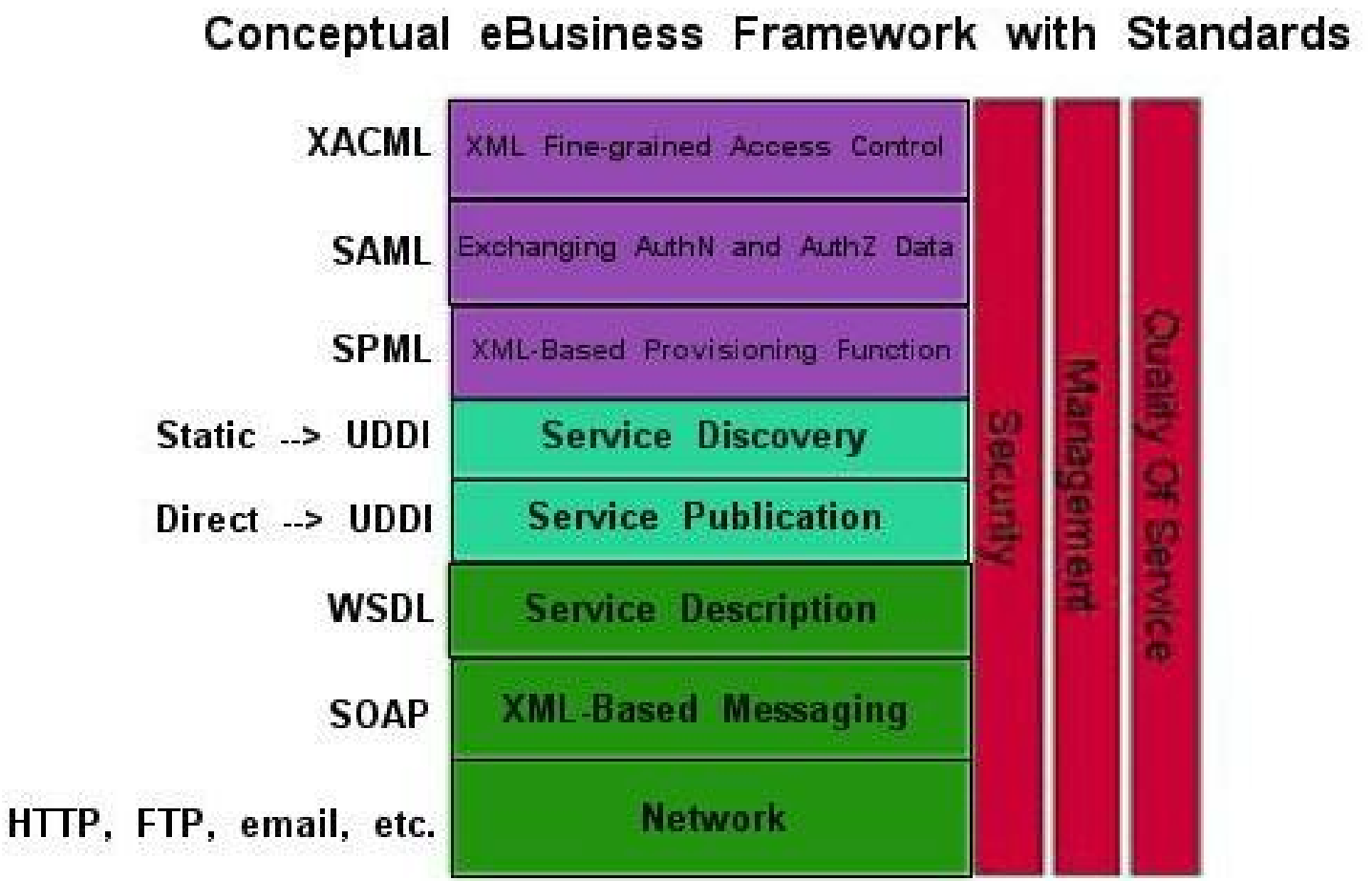
- To address fine grained control of authorized activities
  - In the case of billing a certain activity or allowing a doctor to view a certain part of a patient's medical record (XML-based) which the patient has authorized to view

XKMS – Authentication Services

XKMS - XML-based mechanism for doing PKI

This mechanism, XKMS-based PKI may be used to verify against a certificate to provision a system entity to a service/resource

Conceptual eBusiness Framework with Standards Stack



*Derived From: Gottschalk, Karl; Graham, Steve; Kreger, Heather; and Snell, James. "Introduction to Web Services Architecture." http://www.research.ibm.com/journal/sj/412/gottschalk.html. Emerging Technologies. IBM Software Group. November 2001.

Business Case Issues

A group of organizations who want to do business together need to trust the identities of system entities requesting access to a resource or service

- How does an organization authorize user's of another organization to use the service of the others to conduct business securely?
- What components can be used/reused to provide a seamless single sign-on solution to access web-based and backend resources and services with web services?

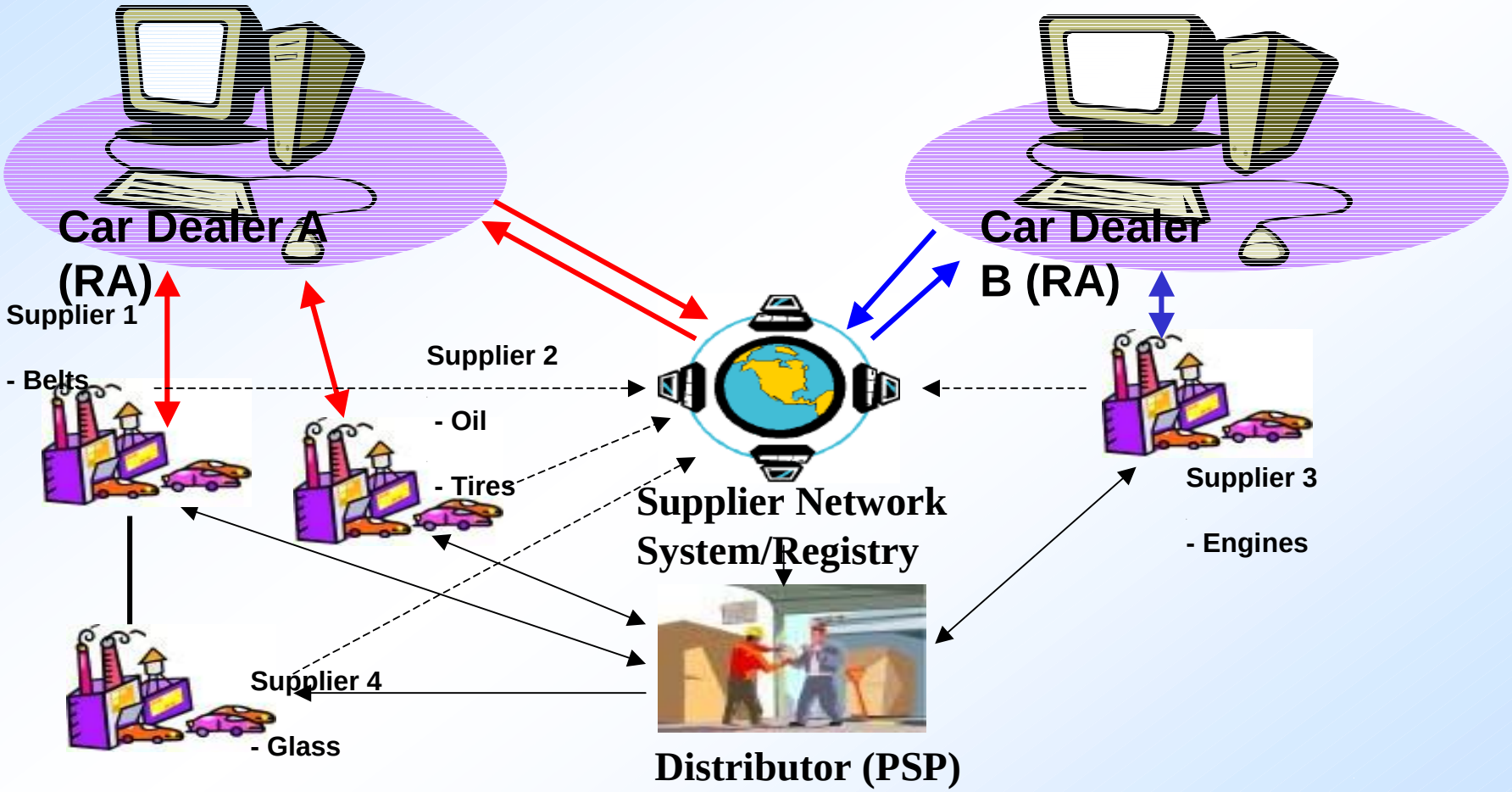
The Business vs. IT Challenge

- IT Orientation: Managing user access in complex environments depends on
  - Well Defined Security Policy
  - Robust Security Enforcement Mechanisms
  - Establishing Identity, Authorization, and Trust
  - Level of ‘automation vs. manual control’
- Business Orientation: Activities / access depend on achieving business goals while meeting
  - Contractual obligations
  - Regulatory and legal requirements

eBusiness Example

- Large Supplier Network providing resources and services to a group of automobile dealerships
  - Simultaneously resell multiple products
  - Primary Sub-contractors continue to sub-contract several layers below themselves
  - A dynamic relationship is generated, via a web service, between the suppliers of the Supplier Network System
- This scenario results in a complex chain of events leading to complex information access requirements from which the system entity must be authorized to use the resource or service based on the authorization attributes...

Supply Chain Complexity



Supply Chain Example Highlights

- Resources and Services are published as web services in a UDDI registry
- (Supplier): The system entity requesting to sell goods is summoned to provide credentials to the authorizer (I.e., Distributor PSP, Provisioning Service Point a.k.a. Policy Enforcement Point [PEP])

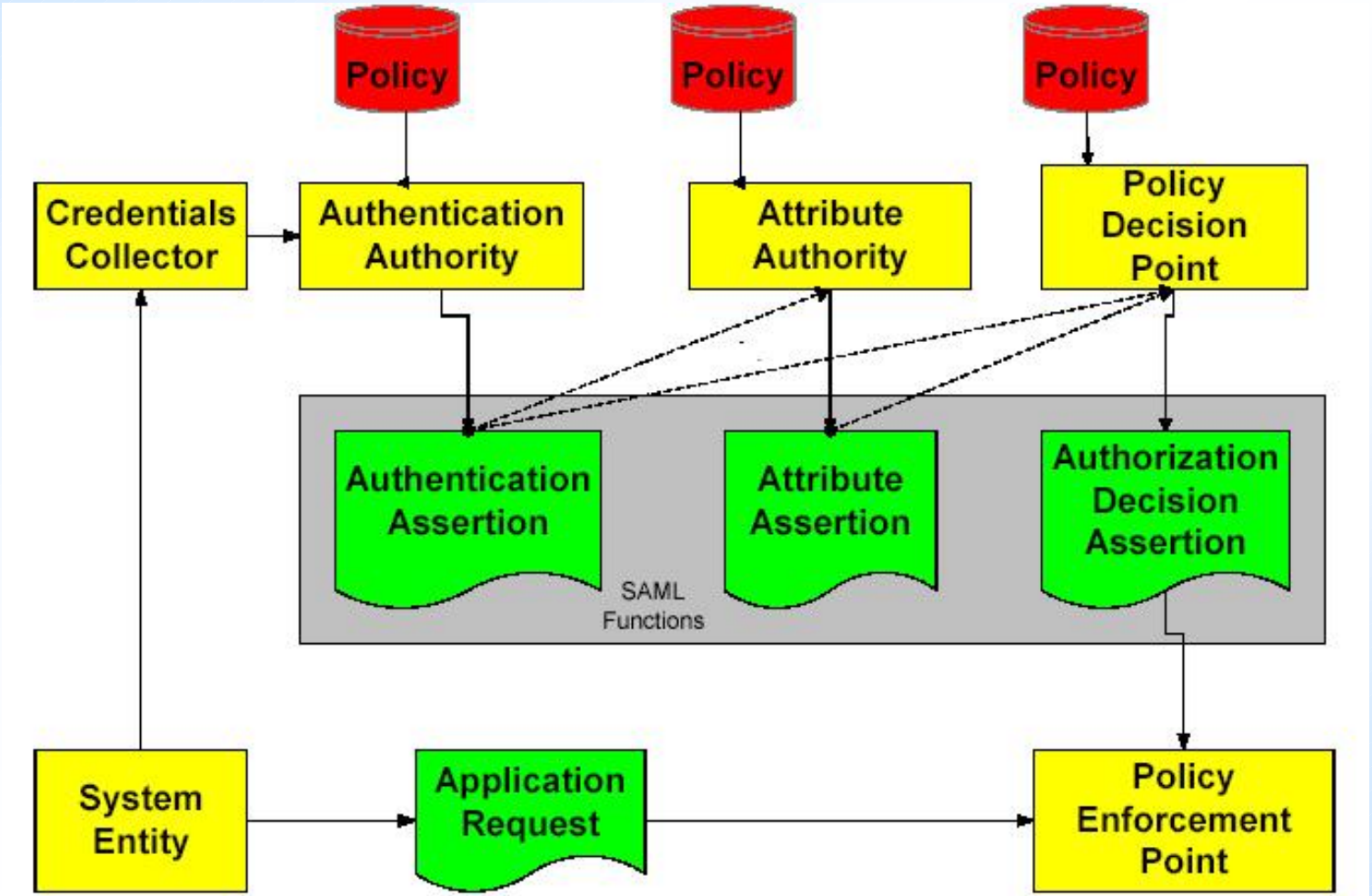
Supply Chain Example Highlights

- (Dealership): The system entity requests to purchase goods based on the fact that the supplier is authorized to sell those goods
- XKMS certificate authority may be used to verify against a certificate to provision that system entity to a service/resource
- Within SAML, the Policy Enforcement Point (the Distributor) of the application, checks permissions against the Policy Decision Point for an Authorization Decision Assertion, whether to allow access for the System Entity to that Application.

Supply Chain Example Highlights

- Within SAML's Policy Enforcement Point (the Distributor) of the application, checks permissions against the Policy Decision Point for an Authorization Decision Assertion, whether to allow access for the System Entity to that Application.

Allowing the System Entity to have Access



Business Requirements relating to Attributes

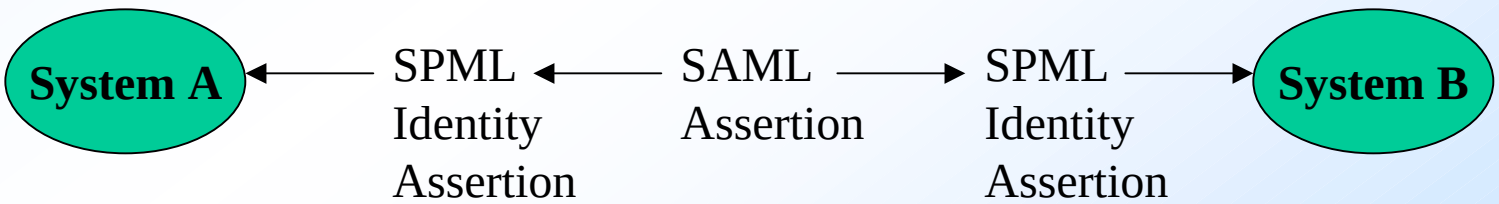
- Supply chain behavior is based on contractual relationships, legal requirements and regulatory conditions…not just security concerns
- Must reflect all parameters of the relationship. For example:
  - Number of users
  - Types of users / # per type
  - Length of stay
  - Access rights
  - Reporting hierarchy
  - Administrative hierarchy
  - Citizenship

Role of Standards

- The role of SAML
  - SAML handles the Identity Information and its attributes across the transaction between parties
  - An authorization service is offered as shown in the diagram above

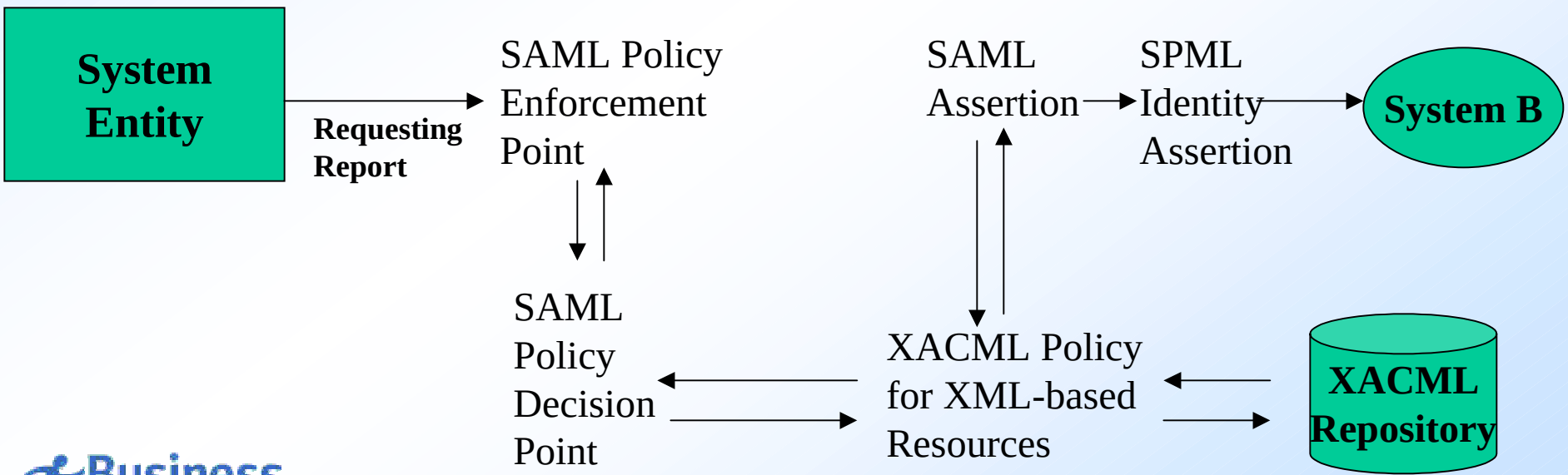
Role of Standards

- The role of SPML
  - SPML, resident on the service provider and requestor's side, does a lookup on the Authorization Decision Assertion from SAML to understand what the system entity is allowed to sell, purchase, lease, or use at resource or service level
  - Conditions considered
    - Systems or Services requesting access for
    - May be IT-based, Billing, Parts (Services), etc…



Role of Standards

- The role of XACML
  - Can Provide Detailed cost of transaction
    - XACML may be used to derive how many transactions were conducted during the month at the XML granular level of the resource or service provided.



Analysis of the Scenario

- Correct account setup for each person at each layer
  - Suppliers can only choose from options assigned by their Distributors authorization according to their credentials.
  - The SAML Authorization Decision Assertion, which tells that the system entity requesting access whether the entity is allowed or denied
  - If allowed, the SAML Authorization Decision Assertion will be passed to the SPML Identity Assertion at the Supplier's endpoint to validate access to the end resource or service.
  - Management
    - **Subscription to the requested service or resource is handled according to above constraints**
    - **Creation and assignment of security mechanisms to users & resources is properly maintained**

Where does Provisioning fit in?

- Suppliers, who may use SPML-compliant applications/services (part of the supplier's endpoint) will validate the access to resources and services on the backend that are requested.
  - Additional functions that will be effects of using interoperable standards are:
    - Full end-to-end Audit trail processes providing consolidated reporting
    - Ability to incorporate Two-Factor Authentication methods to enhance security
    - Administrating the access to those backend resources/services

How will SPML help in the future based on what we have learned?

- Components which may interoperate with SAML request and response
- Delegated administration of digital resources to the extended enterprise
  - e.g., Access to backend resources for supply chain users and external administrators
- Exchange of provisioning requests between users
- Exchange of provisioning request and response between organizations

Collaboration among standards groups

- SSJC (Security Standards Joint Committee)
  - A committee developed within OASIS to promote consistency, interoperability, and re-use across the Technical Committees within OASIS
  - Example of Joint Collaboration may be the idea of SPML, SAML, XACML working together to a joint goal

Final Thought

- SPML is only one component of the pyramid that will allow identities to be managed effectively and for the eBusiness framework to become fluid. Many standards that need to build this scenario are still in development.

For further information

For more information, please visit:

(SPML) http://www.oasis-open.org/committees/spml
(SAML) http://www.oasis-open.org/committees/saml
(XACML) http://www.oasis-open.org/committees/xacml

Business Case Paper may be reviewed at:

http://lists.oasis-open.org/archives/provision/200206/msg00008.html

References

HTTP: http://www.w3.org/Protocols/

SOAP: http://www.w3.org/TR/SOAP/

WSDL: http://www.w3.org/TR/wsdl

UDDI: http://www.uddi.org

ebXML: http://www.ebxml.org

SPML: http://www.oasis-open.org/committees/spml

SAML: http://www.oasis-open.org/committees/saml

XACML: http://www.oasis-open.org/committees/xacml

Gottschalk, Karl; Graham, Steve; Kreger, Heather; and Snell, James. "Introduction to Web Services Architecture." http://www.research.ibm.com/journal/sj/412/gottschalk.html. Emerging Technologies. IBM Software Group. November 2001.

Sodhi, Gavenraj. "Subscription and Identity Management Interoperability ." http://lists.oasis-open.org/archives/provision/200206/msg00008.html. Business Layers. June 2002.

Q&A

Thanks

Business Layers™

The eProvisioning Company™

Thank you

Gavenraj Sodhi

gavenraj.sodhi@businesslayers.com

(201) 757-4090