Security Models

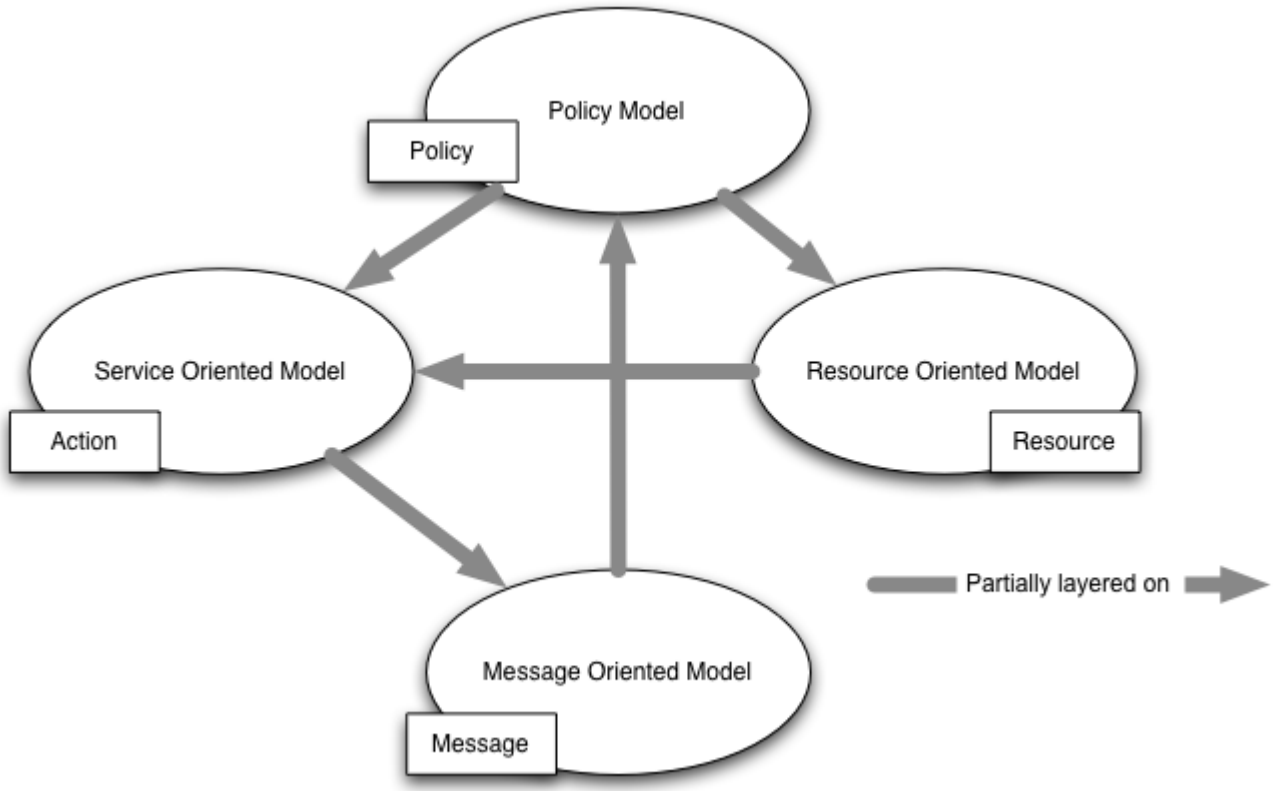
Survey for OsEra

Landscape

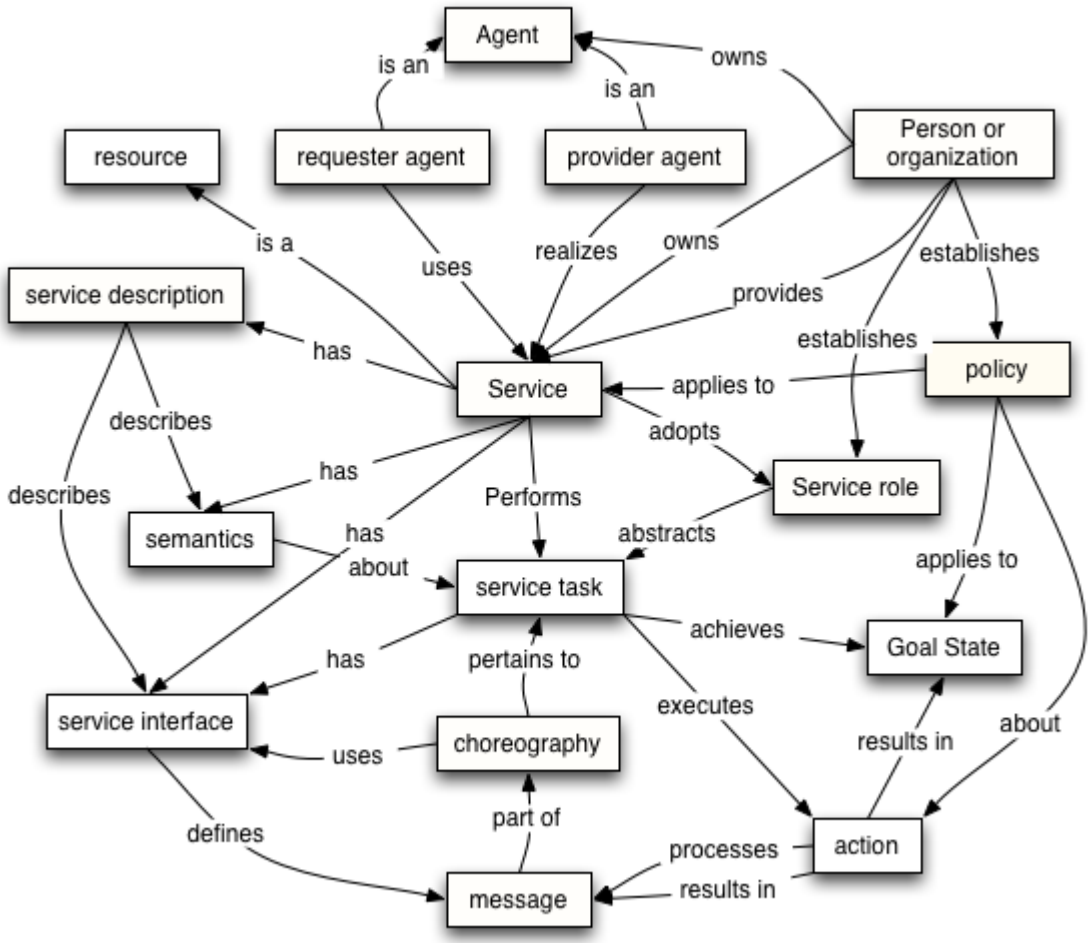
- Permissions (For roles to perform actions)
  - SecureUML
  - OpenPMF
- Identity management
- Trust
- Management frameworks/products/standards
- Assertions & Credentials (SAML)
- Interactions/Process
  - ebXML BPSS/CPPA, Rosettanet
- Web services stack
  - WS-Security, WS-SecurityPolicy, WS-Trust, WS-SecureConversation, WS-Federation, etc…

Web Services Stack

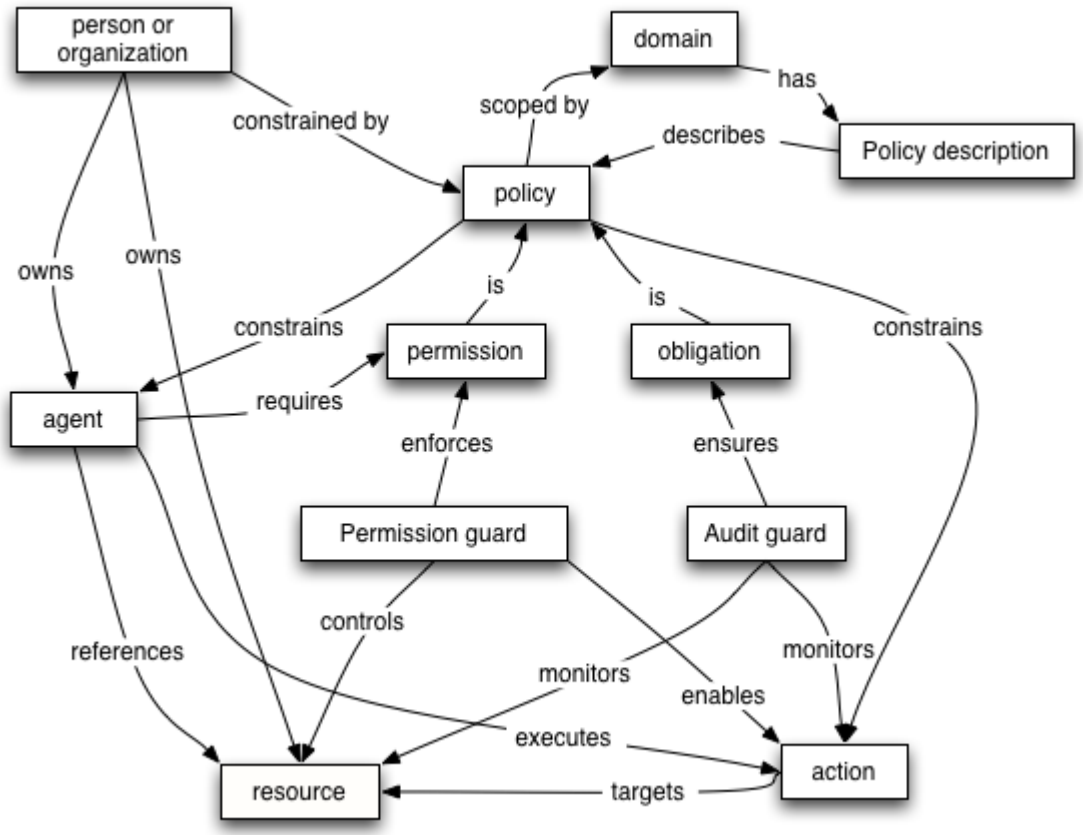
- Web Services Architecture http://www.w3.org/TR/ws-arch/



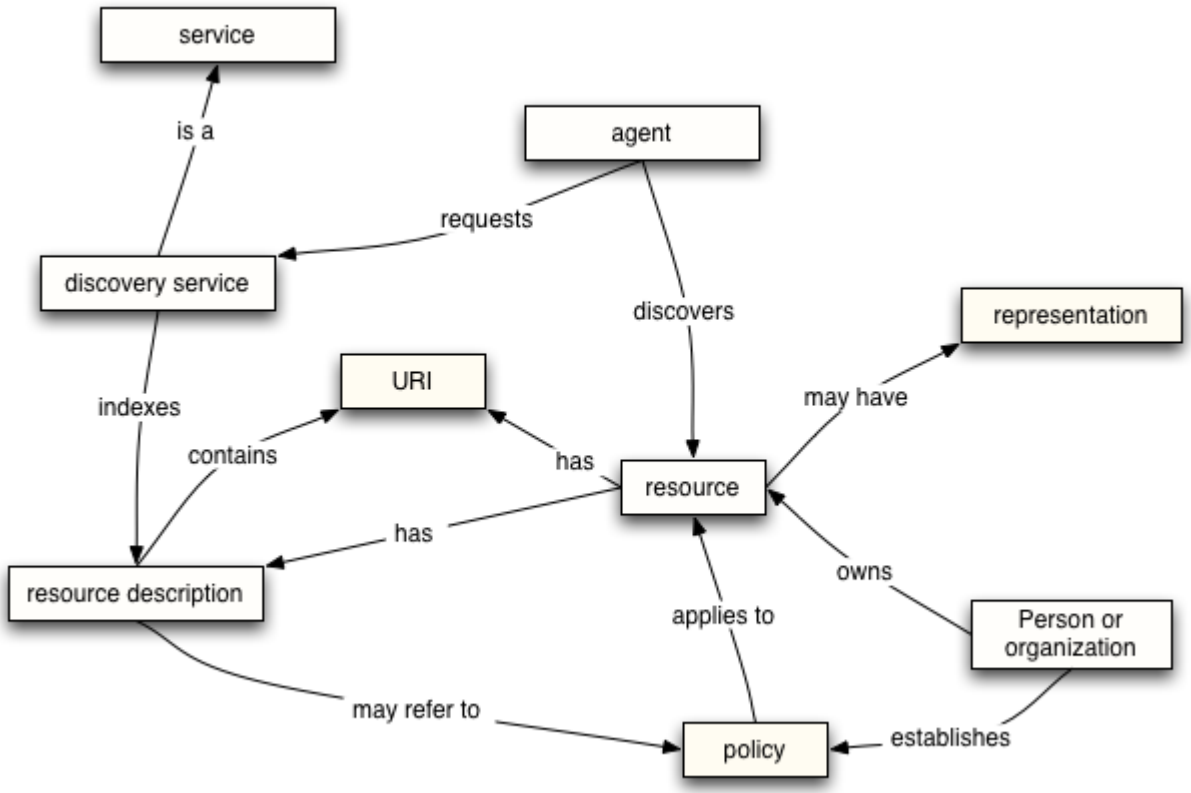
Web services stack “service”



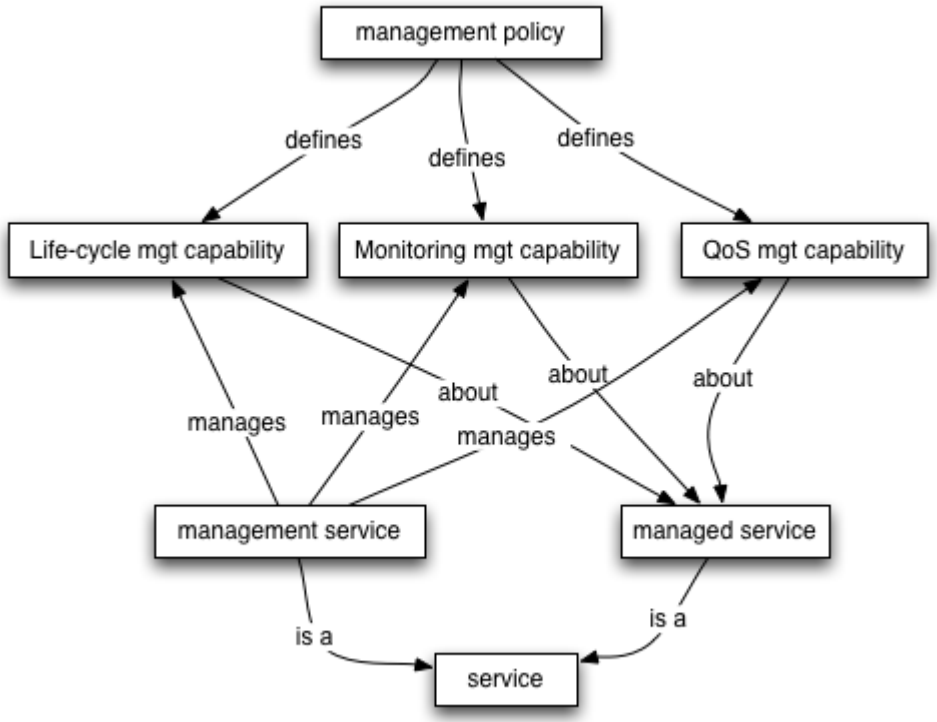
Web services stack policies



Web services stack resources

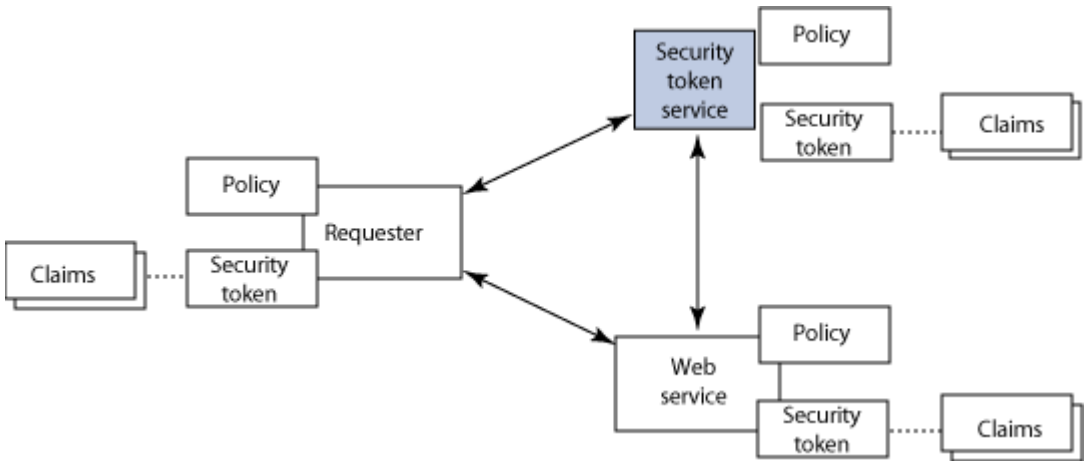


Web services stack - Management



Trust

- IBM- SOA programming model for implementing Web services
- http://www-128.ibm.com/developerworks/webservices/library/ws-soa-progmodel7/



Secure UML

- http://www.sti.uniurb.it/events/fosad05/mdac-tosem.pdf
- http://www.informatik.uni-freiburg.de/~tolo/pubs/p344-lodderstedt.pdf
- http://www.informatik.uni-freiburg.de/~tolo/pubs/secuml_uml2002.pdf

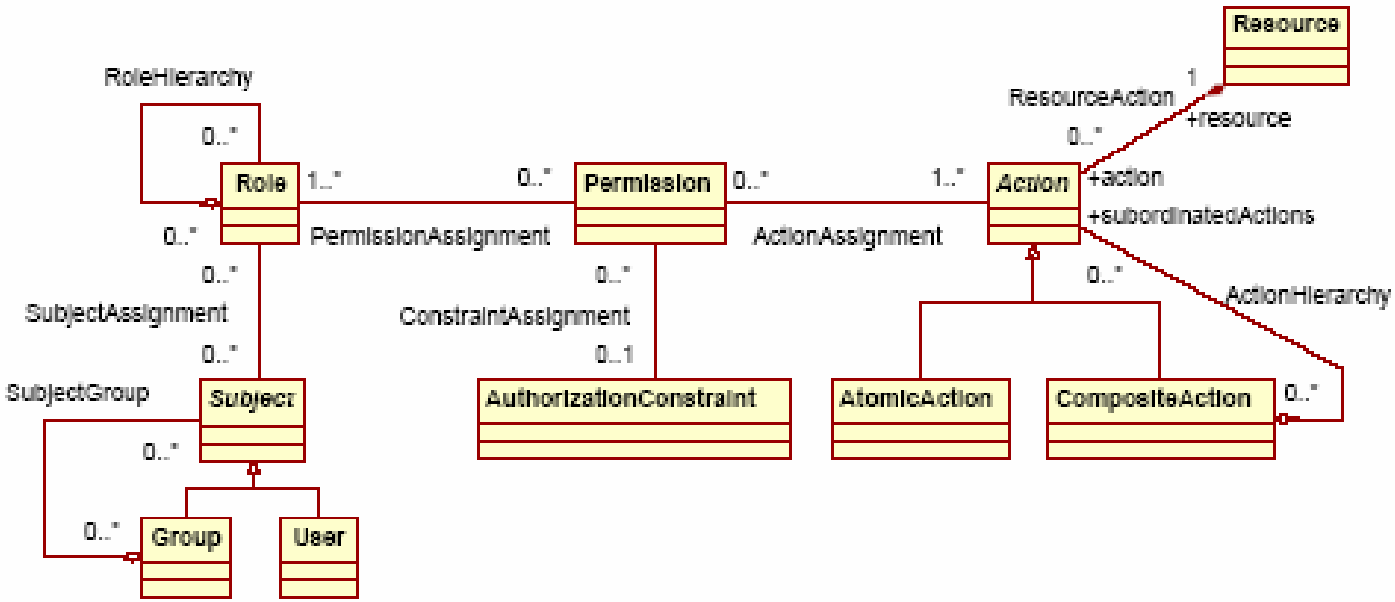
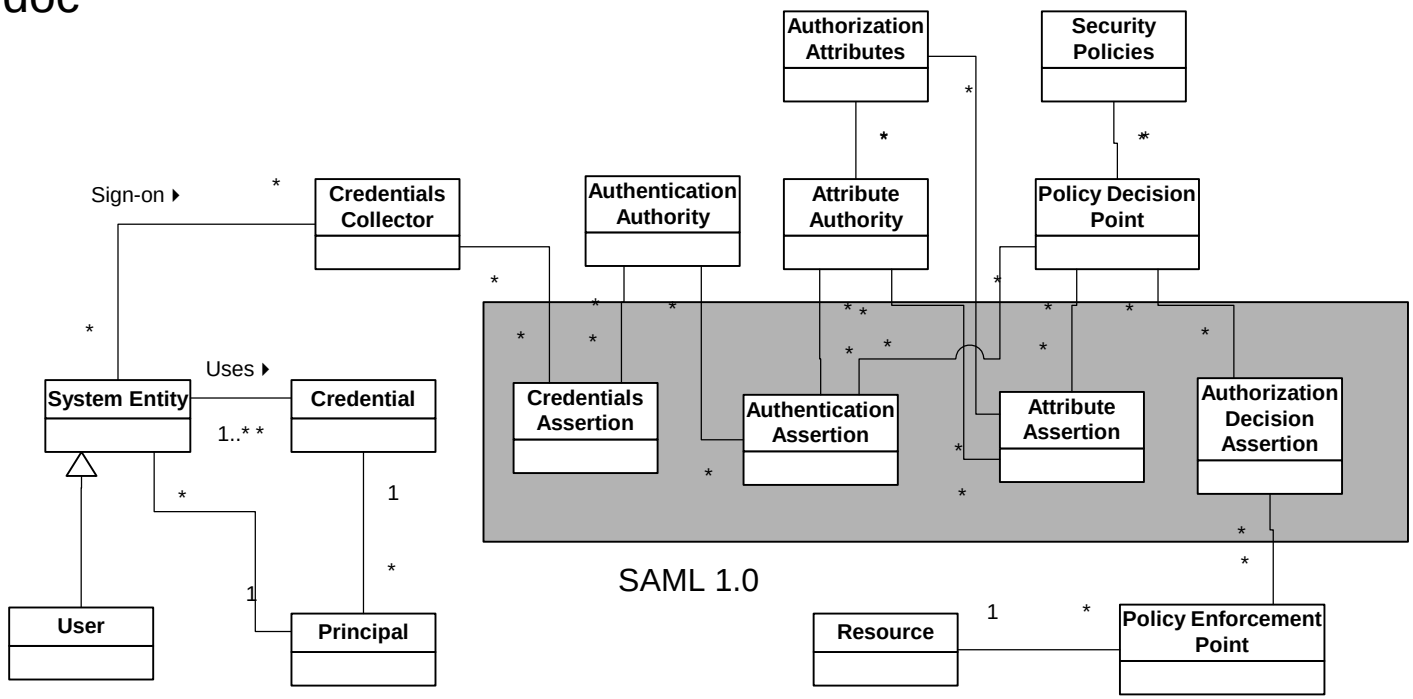


Figure 8: SecureUML metamodel

Identity, Assertions & Credentials

- **SAML Domain model**
- http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20
- http://www.oasis-open.org/committees/security/docs/draft-sstc-use-domain-04.doc

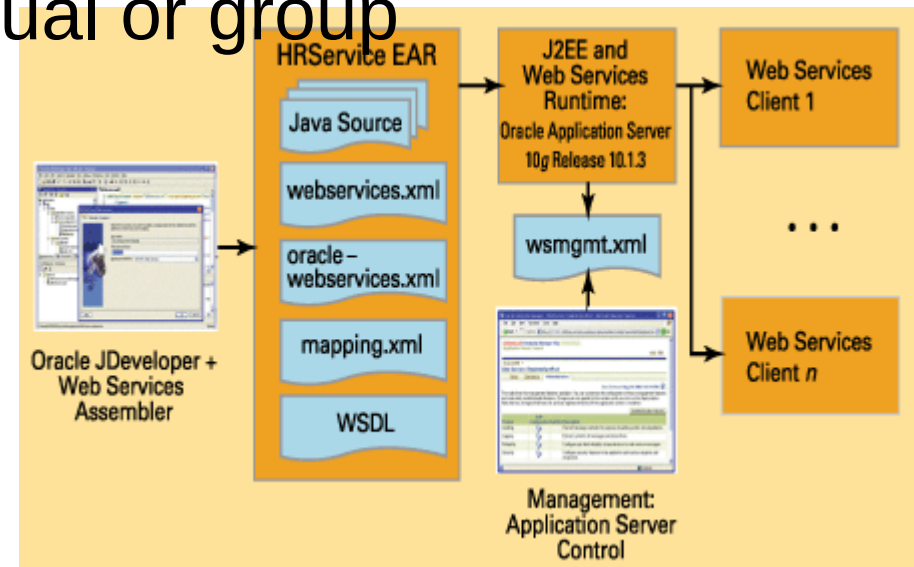


Business Model Semantics

- Identify roles, actions, interactions
  - Already in EDOC
- Role/type based permissions
- Certification types
- Rule types
- Concepts of obligation
  - http://www.w3.org/2004/10/presentations/lalana.ppt#267,13,Rei Specifications
- Requirements of interactions
  - Information Security
    - Confidential, Authenticated, Tamperproof (ebXML, Rosetanet)
  - Secure [trusted] identity
  - Non repudiation (ebXML, Rosetanet)

Administrative/Instance Level

- Individuals, groups & resources [instances]
- Trust
  - Authority
  - Identity
  - Certifications
- Authorization of individual or group
  - To perform in a role
  - To perform a action
  - To utilize resource



Rules/Policies

- Rules about interactions & resources
  - All web service requests from external sources shall have the identity of the requester validated by a trusted authority.
  - All purchase orders require non repudiation to be processed.
  - Credit card numbers will be encrypted.
- Rules about instances combined with process
  - Ex; On work Mondays all members of accounting with a GL-POST certification are authorized to post GL adjusting entries.
- Business rules about technology concerns
  - **Acceptable Encryption Policy**
    - Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec.

Identity Management

- Existing products (I.E. Oracle, MS)
- Web Services Access Control - http://www.oracle.com/products/middleware/identity-management/web-services-access.html
- Press - http://news.zdnet.com/2100-1009_22-5535345.html
- Ws-federation - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/wsfedinterop.asp

- Note; this will probably be a service to us

jBoss

- The JBoss Security Model
  - http://www.huihoo.com/jboss/online_manual/3.0/ch09s08.html
- jBoss security
  - http://www.jboss.org/developers/projects/jboss/security
- jBoss SAML project
  - http://www.jboss.com/?module=bb&op=viewtopic&t=65177

Initial Conclusions

- Very complex area with a lot going on, lots of existing stuff
- What we need in the OsEra meta model
  - Concept of permission joining existing concepts of roles, actors and actions
  - Requirements of interactions (Aspects of protocols/flows)
    - Information Security
      - Confidential, Authenticated, Tamperproof (ebXML, Rosetanet)
    - Secure [trusted] identity
    - Non repudiation (ebXML, Rosetanet)
- What we need at runtime
  - Ws-Security & SAML implemented in our application server
  - Then there is “bind time” – E.G. CPPA
- Systems management
  - There is also need for support at “systems management time” – this is where many policies are defined. Existing vendors will populate this space (**Oracle-eb Services Management Arrives)** . *But, they need to be able to reference the model for roles, activities, actor types and resources.*
- We will use a security service (Trusted 3rd party) supported by the management platforms

References

- A Flexible, Model-driven Security Framework for Distributed Systems - http://www.actapress.com/PaperInfo.aspx?PaperID=20367
- Web Services Security Specifications Index Page - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/wssecurspecindex.asp
- Open PMF - http://www.objectsecurity.com/openpmf/openpmf.html,
- Modeling Security Concerns in Service-Oriented Architectures - http://www-128.ibm.com/developerworks/rational/library/4994.html
- The SANS Security Policy Project - http://www.sans.org/resources/policies/
- Modeling Security Concerns in Service-Oriented Architectures - http://www-128.ibm.com/developerworks/rational/library/4994.html
- Declarative policies for web services - http://www.w3.org/2004/10/presentations/lalana.ppt#256,1,
- Dynamic middleware - http://www.seas.gwu.edu/~shmuel/CMPLX/Dynamic%20Middleware%20for%20Complex%20Organizations.ppt#256,1,
- Dynamic Middleware for Complex Organizational Systems (Dymacos) - http://www.seas.gwu.edu/~shmuel/CMPLX/Dynamic%20Middleware%20for%20Complex%20Organizations.ppt#278,19,Meta-Policies%20for%20Distributed%20Role-Based%20Access%20Control%20Systems
- Policy Management for the Web - http://cs.umbc.edu/pm4w/
- Web Services Management Arrives (Oracle) - http://www.oracle.com/technology/oramag/oracle/04-nov/o64web.html
- IBM Web Services Security http://www-128.ibm.com/developerworks/webservices/library/specification/ws-secure/

References Mindswap

- Web Services Policy Project - http://www.mindswap.org/2005/services-policies/
  - Policy-> OWL XSLT; http://www.mindswap.org/2005/services-policies/wsp2owl.xsl
- Representing Web Service Policies in OWL-DL - http://www.mindswap.org/papers/2005/Policy-ISWC05.pdf
- Expressing WS Policies in OWL - http://www.mindswap.org/papers/2005/WSPolicyInOWL.pdf
- Towards a Policy-Aware Web - http://www.cs.umbc.edu/swpw/papers/kolovski.pdf

Messaging – ebXML/ Rosettanet

- ebXML BPSS - http://www.oasis-open.org/committees/documents.php?wg_abbrev=ebxml-bp
- ebXML CPPA/CPPP- http://www.oasis-open.org/committees/ebxml-cppa/documents/ebCPP-2_1.pdf
- Rosettanet - http://e-docs.bea.com/wli/docs81/tpintro/RNSec_appx.html

References – Secure UML

- Model Driven Security: from UML Models to Access Control Infrastructures – http://www.sti.uniurb.it/events/fosad05/mdac-tosem.pdf
- Model Driven Security for Process Oriented Systems - http://www.informatik.uni-freiburg.de/~tolo/pubs/p344-lodderstedt.pdf
- SecureUML: A UML-Based Modeling Language for Model-Driven Security - http://www.informatik.uni-freiburg.de/~tolo/pubs/secuml_uml2002.pdf

Security/Policy Management

- Xtradyne Security Policy Server - http://www.prismtechnologies.com/section-item.asp?sid4=&sid3=164&sid2=27&sid=18&id=332
- Security Configuration Wizard in Windows Server 2003 - http://www.windowsecurity.com/articles/Security-Configuration-Wizard-Windows-Server-2003-SP1.html
- Web Services Management Arrives (Oracle) - http://www.oracle.com/technology/oramag/oracle/04-nov/o64web.html
- http://www.managedmethods.com/
- http://www.forumsys.com/SOA_Citi_Webinar.htm
- Web Services Management Framework - http://devresource.hp.com/drc/specifications/wsdm/index.jsp
- http://www.w3.org/2002/ws/arch/4/management/

Policy Engines

- http://www.bnx.com/web/solutions/auth/policy_engine.htm
- http://www.novell.com/partnerguide/product/100329.html
- http://www.mindswap.org/2005/services-policies/

Preliminary Business Security Model