JBoss Security For JEMS Technologies

-Anil Saldhana & Scott Stark
JBoss Inc.

Speaker Introduction

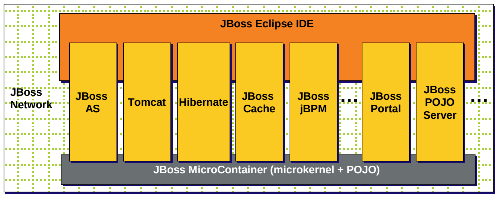
- Anil Saldhana is a member of R & D organization at JBoss.
- Scott Stark is the cofounder of JBoss Inc and is currently the VP of Technology and Integration.

Agenda

- JEMS Architecture
- Authentication Infrastructure
  - ✓ Externalized Tomcat Authenticators
  - ✓ JSR-196 [Java Authentication SPI for containers]
- Authorization Infrastructure
  - ✓ XACML Use Case – JBoss Portal
  - ✓ Policy based framework (JACC, XACML, WS-Policy).
- Roadmap + Future Possibilities
- Demo / Q & A

JEMS Architecture

- Security is a cross-cutting concern

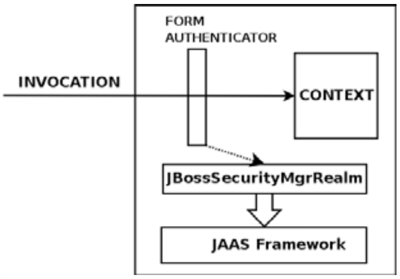


Authentication Infrastructure

- Externalization of Tomcat Authenticators
  - ✓ since jboss-4.0.4.GA
  - ✓ key feature for customizing TC security
    - Handle federation, header based auth etc.
      - ✓ adapt existing standard authenticators
    - Control callout to Tomcat Realms

Authentication Infrastructure

- Externalization of Tomcat Authenticators



Authentication Infrastructure

- JSR-196 [Java Authentication SPI for Containers]
  - ✓ Pros:
    - Allows us to have a notion of container messages during authentication, unlike the current JAAS based infrastructure in JBoss.
      - ✓ Servlets – HttpServletRequest/HttpServletResponse
  - ✓ Cons:
    - Specification is in Draft Stage.
      - ✓ Targeted for JEE6.

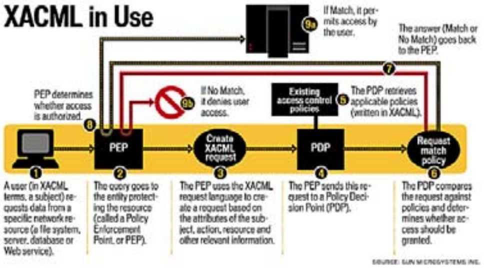
Authorization Infrastructure

- Much more difficult space to solve than the authentication space.
- Current:
  - ✓ JACC - only mandated spec in JEE world.
  - ✓ JEE RBAC with DD (web.xml,ejb-jar.xml) is limited for JEMS projects like portal.
- Future:
  - ✓ Potential suitors for solutions are XACML, WS-Policy etc.

Authorization Infrastructure

- XACML (eXtensible Access Control Markup Language)
  - ✓ OASIS Standard.
  - ✓ Rich Language for Access Control.
    - Can use all available information for access decision- resource properties, environmental conditions (date/time/location) and subject attributes.
  - ✓ Cons:
    - Creating/editing XACML Policy Files is difficult with no good editors/tools.

Authorization Infrastructure


XACML in Use
9a
If Match, it permits access by the user.
The answer (Match or No Match) goes back to the PEP.
7
PEP determines whether access is authorized.
8
9b
If No Match, it denies user access.
Existing access control policies
5
The PDP retrieves applicable policies (written in XACML).
PEP
Create XACML request
PDP
Request match policy
1
A user (in XACML terms, a subject) requests data from a specific network resource (a file system, server, database or Web service).
2
The query goes to the entity protecting the resource (called a Policy Enforcement Point, or PEP).
3
The PEP uses the XACML request language to create a request based on the attributes of the subject, action, resource and other relevant information.
4
The PEP sends this request to a Policy Decision Point (PDP).
6
The PDP compares the request against policies and determines whether access should be granted.

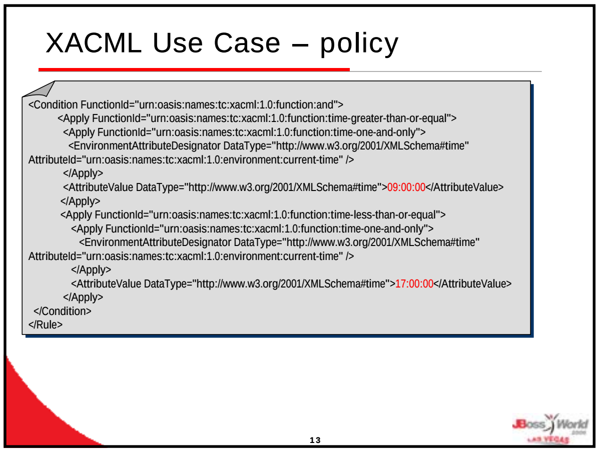
SOURCE: SUN MICROSYSTEMS INC.

Authorization Infrastructure

- XACML Use Case for JBoss Portal
  - ✓ Define the policy as follows:
    - /companyportal
      - ✓ portal accessible between 9am and 5pm
    - /companyportal/EighteenYearOld
      - ✓ portal page accessible only if age == 18 years

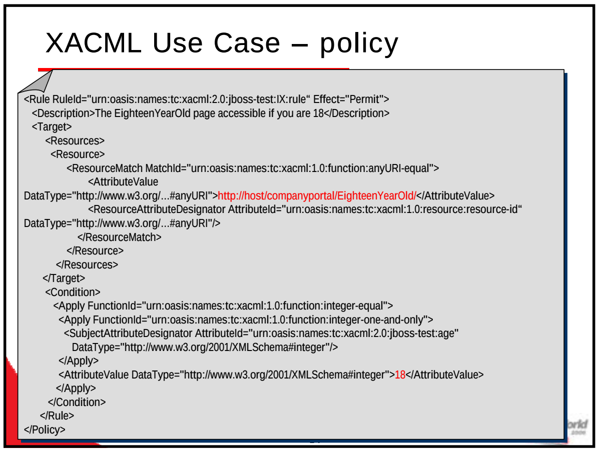
XACML Use Case – policy

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi=“…“  xsi:schemaLocation=“….“ PolicyId=“…"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
  <Description>Policy for Portal Use Case.</Description>
  <Target/>
  <Rule RuleId="urn:oasis:names:tc:xacml:2.0:test:II:rule“ Effect="Permit">
    <Description>Portal accessible between 9 am and 5pm</Description>
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://host/companyportal/</AttributeValue>
            <ResourceAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
          </ResourceMatch>
        </Resource>
      </Resources>
     </Target>
```



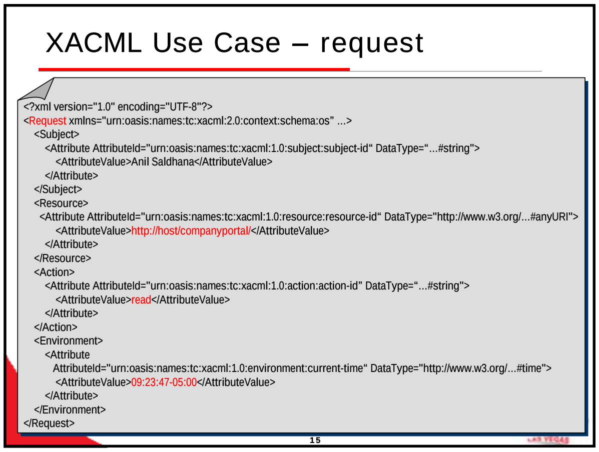
XACML Use Case – policy

```
<Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
              <EnvironmentAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#time"
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" />
            </Apply>
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
           </Apply>
           <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal">
               <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
                  <EnvironmentAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#time"
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" />
               </Apply>
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
            </Apply>
  </Condition>
</Rule>
```



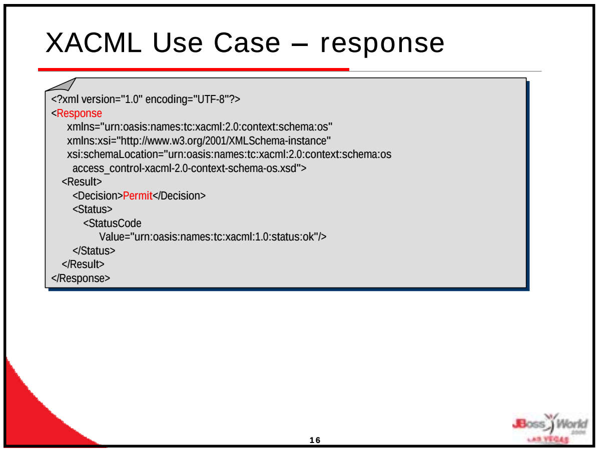
XACML Use Case – policy

```
<Rule RuleId="urn:oasis:names:tc:xacml:2.0:jboss-test:IX:rule“ Effect="Permit">
   <Description>The EighteenYearOld page accessible if you are 18</Description>
   <Target>
        <Resources>
          <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                        <AttributeValue
DataType="http://www.w3.org/...#anyURI">http://host/companyportal/EighteenYearOld/</AttributeValue>
                        <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id“
DataType="http://www.w3.org/...#anyURI"/>
                    </ResourceMatch>
                </Resource>
            </Resources>
       </Target>
        <Condition>
           <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
             <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
               <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:jboss-test:age"
                  DataType="http://www.w3.org/2001/XMLSchema#integer"/>
             </Apply>
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">18</AttributeValue>
            </Apply>
         </Condition>
      </Rule>
</Policy>
```



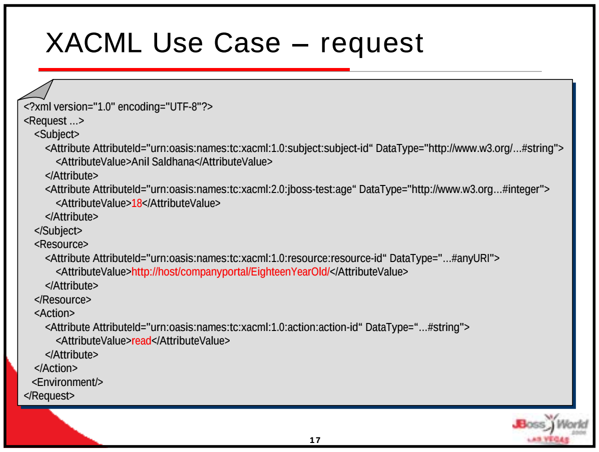
XACML Use Case – request

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os” ...>
   <Subject>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id“ DataType=“...#string">
         <AttributeValue>Anil Saldhana</AttributeValue>
      </Attribute>
   </Subject>
   <Resource>
     <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id“ DataType="http://www.w3.org/...#anyURI">
         <AttributeValue>http://host/companyportal/</AttributeValue>
      </Attribute>
   </Resource>
   <Action>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id” DataType=“...#string">
         <AttributeValue>read</AttributeValue>
      </Attribute>
   </Action>
   <Environment>
      <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time“ DataType="http://www.w3.org/...#time">
         <AttributeValue>09:23:47-05:00</AttributeValue>
      </Attribute>
   </Environment>
</Request>
```



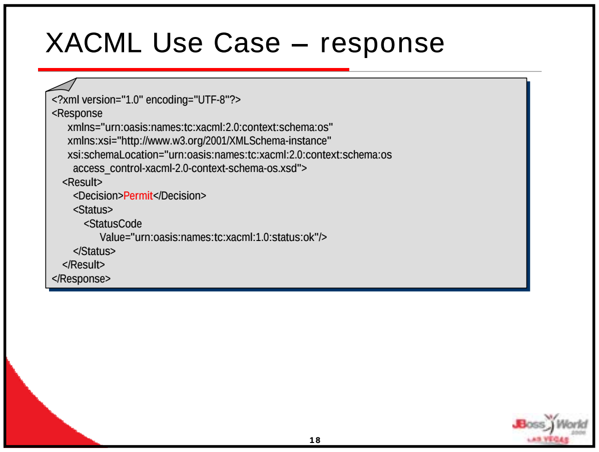
XACML Use Case – response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response
     xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
      access_control-xacml-2.0-context-schema-os.xsd">
   <Result>
      <Decision>Permit</Decision>
      <Status>
         <StatusCode
            Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
      </Status>
   </Result>
</Response>
```



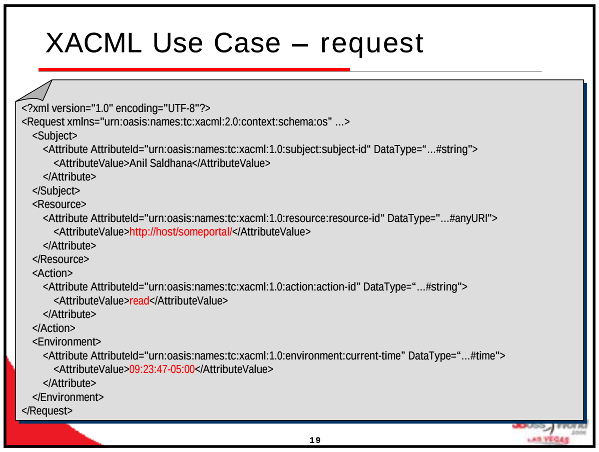
XACML Use Case – request

```
<?xml version="1.0" encoding="UTF-8"?>
<Request ...>
   <Subject>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id“ DataType="http://www.w3.org/...#string">
         <AttributeValue>Anil Saldhana</AttributeValue>
      </Attribute>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:jboss-test:age“ DataType="http://www.w3.org...#integer">
         <AttributeValue>18</AttributeValue>
      </Attribute>
   </Subject>
   <Resource>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id“ DataType="...#anyURI">
         <AttributeValue>http://host/companyportal/EighteenYearOld/</AttributeValue>
      </Attribute>
   </Resource>
   <Action>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id“ DataType=“...#string">
         <AttributeValue>read</AttributeValue>
      </Attribute>
   </Action>
  <Environment/>
</Request>
```



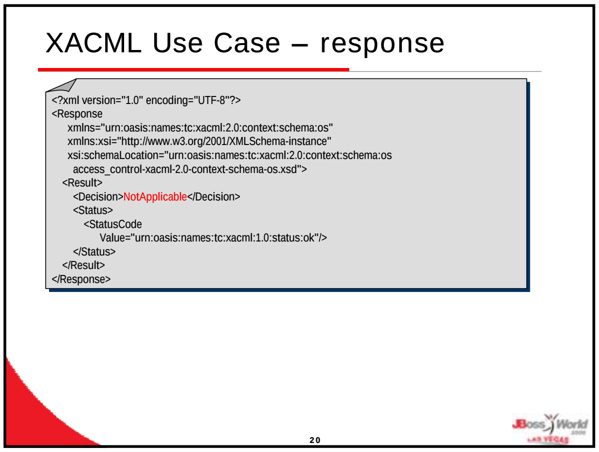
XACML Use Case – response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response
     xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
      access_control-xacml-2.0-context-schema-os.xsd">
   <Result>
      <Decision>Permit</Decision>
      <Status>
         <StatusCode
            Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
      </Status>
   </Result>
</Response>
```



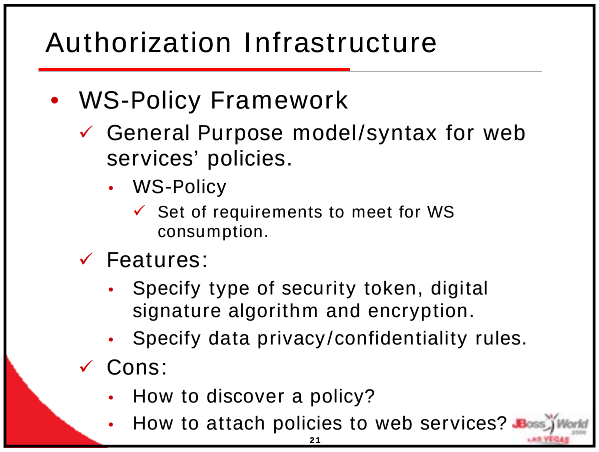
XACML Use Case – request

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os" ...>
   <Subject>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id“ DataType=“...#string">
         <AttributeValue>Anil Saldhana</AttributeValue>
      </Attribute>
   </Subject>
   <Resource>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id“ DataType="...#anyURI">
         <AttributeValue>http://host/someportal/</AttributeValue>
      </Attribute>
   </Resource>
   <Action>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id” DataType=“...#string">
         <AttributeValue>read</AttributeValue>
      </Attribute>
   </Action>
   <Environment>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time” DataType=“...#time">
         <AttributeValue>09:23:47-05:00</AttributeValue>
      </Attribute>
   </Environment>
</Request>
```



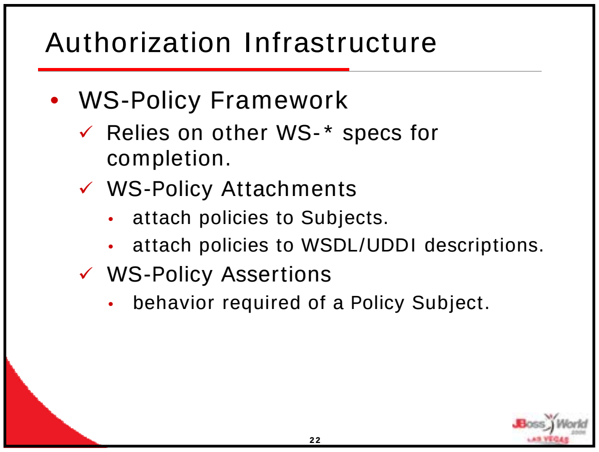
XACML Use Case – response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response
     xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
       access_control-xacml-2.0-context-schema-os.xsd">
   <Result>
      <Decision>NotApplicable</Decision>
      <Status>
         <StatusCode
              Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
      </Status>
   </Result>
</Response>
```



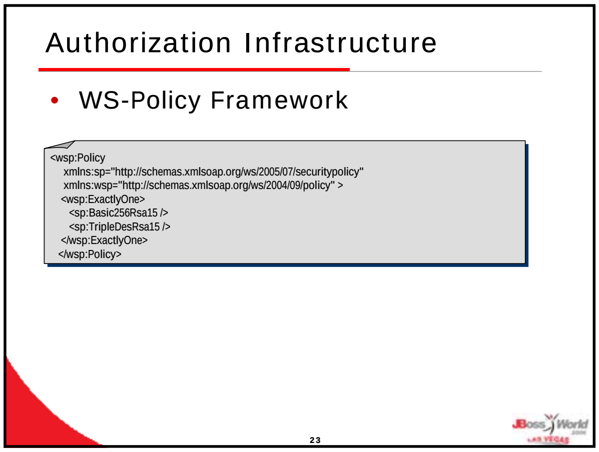
Authorization Infrastructure

- WS-Policy Framework
  - ✓ General Purpose model/syntax for web services’ policies.
    - WS-Policy
      - ✓ Set of requirements to meet for WS consumption.
  - ✓ Features:
    - Specify type of security token, digital signature algorithm and encryption.
    - Specify data privacy/confidentiality rules.
  - ✓ Cons:
    - How to discover a policy?
    - How to attach policies to web services?



Authorization Infrastructure

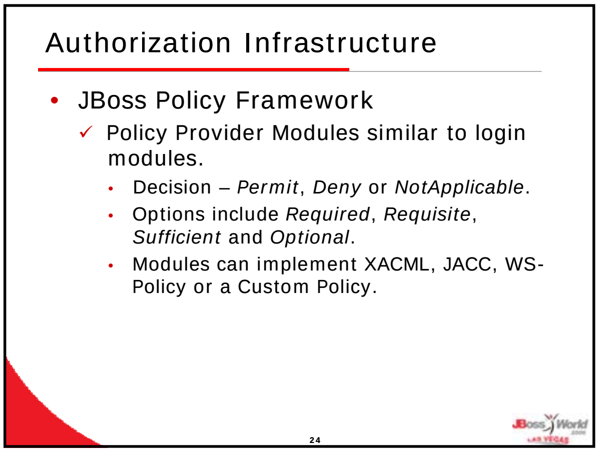
- WS-Policy Framework
  - ✓ Relies on other WS-* specs for completion.
  - ✓ WS-Policy Attachments
    - attach policies to Subjects.
    - attach policies to WSDL/UDDI descriptions.
  - ✓ WS-Policy Assertions
    - behavior required of a Policy Subject.



Authorization Infrastructure

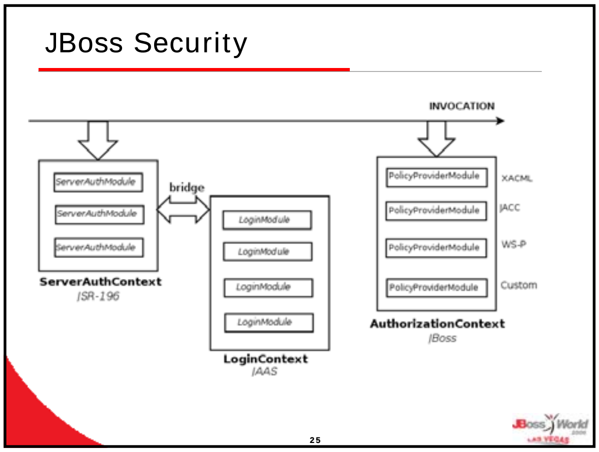
- WS-Policy Framework

```
<wsp:Policy
    xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
    xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" >
   <wsp:ExactlyOne>
     <sp:Basic256Rsa15 />
     <sp:TripleDesRsa15 />
   </wsp:ExactlyOne>
  </wsp:Policy>
```

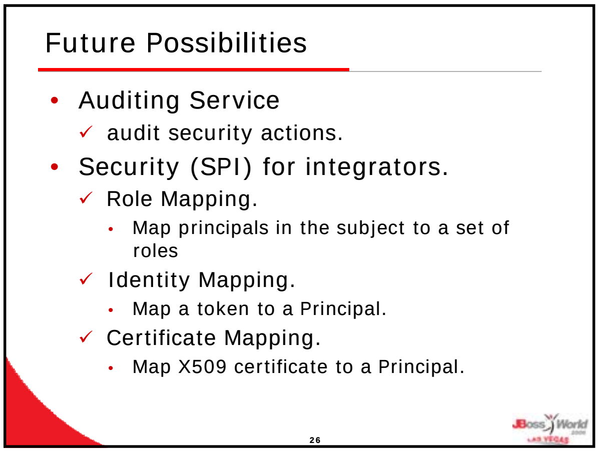


Authorization Infrastructure

- JBoss Policy Framework
  - ✓ Policy Provider Modules similar to login modules.
    - Decision – *Permit*, *Deny* or *NotApplicable*.
    - Options include *Required*, *Requisite*, *Sufficient* and *Optional*.
    - Modules can implement XACML, JACC, WS-Policy or a Custom Policy.

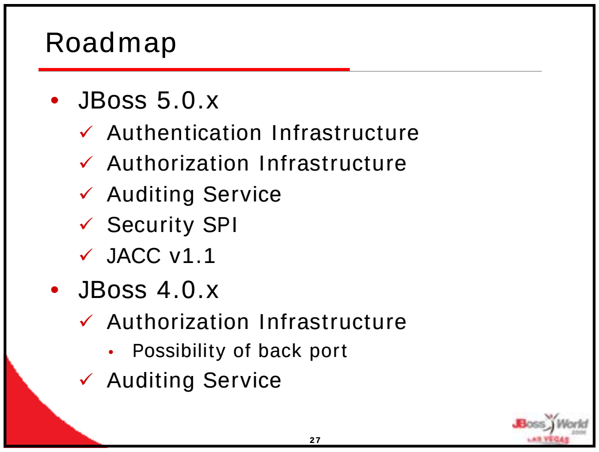


JBoss Security



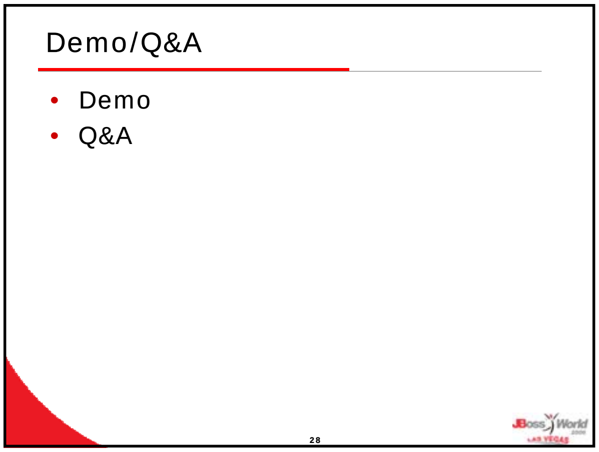
Future Possibilities

- Auditing Service
  - ✓ audit security actions.
- Security (SPI) for integrators.
  - ✓ Role Mapping.
    - Map principals in the subject to a set of roles
  - ✓ Identity Mapping.
    - Map a token to a Principal.
  - ✓ Certificate Mapping.
    - Map X509 certificate to a Principal.



Roadmap

- JBoss 5.0.x
  - ✓ Authentication Infrastructure
  - ✓ Authorization Infrastructure
  - ✓ Auditing Service
  - ✓ Security SPI
  - ✓ JACC v1.1
- JBoss 4.0.x
  - ✓ Authorization Infrastructure
    - Possibility of back port
  - ✓ Auditing Service



Demo/Q&A

- Demo
- Q&A