4. Each provider must satisfy all of the authorization requirements of
the EJB and Servlet specifications corresponding to the target
platform. The provider is not required to satisfy the authorization
requirements pertaining to any of the above specifications for
which the target platform is not a compatible implementation.

5. The evaluation of a permission corresponding to a resource must
identify the context of the resource's use such that different policy
can be applied to a resource used in different contexts (that is,
applications or instances of an application).

6. In the case of Servlet resources, the provider must be able to
associate a distinct policy context with each context root
(including context roots created to support virtual hosting) hosted
by the server.

7. In protecting Servlet resources, a provider must select the policy
statements that apply to a request according to the constraint
matching and servlet mapping rules defined by the Servlet
specification.

8. To support this contract in a Servlet environment, a container or its
deployment tools must create policy statements as necessary to
support Servlet’s “default role-ref semantic”.

9. For a container to support this contract, it must execute in an
environment controlled by a Java SE SecurityManager. Containers
may also execute in environments that are not controlled by a Java
SE SecurityManager. Section 1.5, “Running Without a
SecurityManager” defines changes to this contract that apply to
containers running without a Java SE SecurityManager.

10. Policy providers must perform the permission evaluations
    corresponding to container pre-dispatch decisions and application
    embedded privilege tests (i.e., isUserInRole and isCallerInRole)
    without requiring that containers establish particular values for
    any of the non-principal attributes of the one or more
    java.security.ProtectionDomain objects that are the subject of the
evaluation.

1.4.1 Non Requirements

1. This JSR does not require that containers support server-side
authentication module plug-ins for the purpose of populating
subjects with authorization provider specific principals.

2. This JSR does not require that subjects be attributed with role
principals as a result of authentication.