constructed with principals. The checked permission is granted if Policy.implies returns true. Otherwise, the permission is not granted.

- The J2EE 1.4 container calls `java.security.Policy.getPermissions` with a ProtectionDomain that need not be constructed with principals. The container must call the `implies` method on the returned PermissionCollection using the permission being checked as argument. The checked permission is granted if the PermissionCollection implies it. Otherwise, the permission is not granted. This technique is supported but not recommended.

- The J2EE 1.3 container calls `javax.security.auth.Policy.getPermissions` to determine the collection of permissions granted independent of AccessControlContext. The Subject in the call to `getPermissions` may be null. The container must call the `implies` method on the returned PermissionCollection using the permission being checked as argument. The checked permission is granted if the PermissionCollection implies it. Otherwise, the permission is not granted. This technique is supported but not recommended.

Prior to using any of the techniques described in this section, the container must have established a policy context identifier as defined in Section 4.6, “Setting the Policy Context”.

4.8 Checking the Caller for a Permission

A container must determine if the caller has been granted a permission by evaluating the permission in the context of an AccessControlContext, ProtectionDomain, or Subject containing the principals of (only) the caller[1]. If the caller’s identity has been asserted or vouched for by a trusted authority (other than the caller), the principals of the authority must not be included in the principals of the caller. A container must use one of the following techniques to determine if a permission has been granted to the caller.

- The container calls `AccessControlContext.checkPermission` with the permission as argument. The call to `checkPermission` must be made on

[1] Section 4.12, “Optimization of Permission Evaluations" allows containers to reuse granted results obtained for unauthenticated callers (i.e. with no principals) to authorize, independent of caller identity, permissions implied by such results.