

with a policy type named “performance management” associated with their role. In this example, the role named “manager” has a pre-defined context parameter of “client.” Therefore, the “client” pre-defined context parameter is required in order to assign one or more users to the role of “manager” and to determine one or more policy instances for the “performance management” policy type. In this example, the following “manager” role assignments could be included: user=“Alice” **701**, role=“manager” **703**, and context=“XYZ Client” **704**; and user=“Bob” **702**, role=“manager” **703**, and context=“ABC Client” **705**. In this example, the “performance management” policy type associated with the “manager” role includes policy elements such as “access performance management application,” “view compensation data,” “can increase salary,” and “maximum salary increase percentage.” In this example, a policy instance **706** would apply to “Alice” **701** in her “manager” role **703** based upon the “XYZ Client” pre-defined context parameter **704**. A policy instance **707** would apply to “Bob” **702** in his “manager” role **703** based upon the “ABC Client” pre-defined context parameter **705**. For this example, there are two policy instances, **706** and **707**, for the “performance management” policy type. In this example, the following “performance management” policy instances are illustrated for the role of “manager” **703**: user=“Alice” **701**, “context=“XYZ Client” **704**, access performance management application=“yes” **708a**, view compensation data=“yes” **708b**, can increase salary=“no” **708c**, and maximum salary increase percentage=“0%” **708d**; and user=“Bob” **702**, context=“ABC Client” **705**, access performance management application=“yes” **709a**, view compensation data=“yes” **709b**, can increase salary=“yes” **709c**, and maximum salary increase percentage=“5%” **709d**. In this example, although both users, “Bob” **702** and “Alice” **701**, have the same role **703**, the pre-defined context parameter values of the role assignment for each of them differs. As a result, the policy instances for each user will differ, and in turn, view, access, and update permissions will differ for “Bob” **702** and “Alice” **701**, even though they both are associated with the role of “manager” **703**. In this example, Bob, as a manager within the ABC Client organization, can increase salaries by no more than 5%; whereas, Alice, as a manager within the XYZ Client organization, cannot increase salaries.

[0053] As has been illustrated, the creation of one or more policy instances, associated with the role of a user, one or more pre-defined context parameters, and one or more policy types, can provide for the contextual customization and determination of access rights to one or more resources for different users with the same role.

[0054] The code that follows is exemplary of the method described in FIG. 3 for role-based access in a multi-customer computing environment. In this example, a user **110** named “Inga,” who is an independent contractor, logs on to a computer system **301**. Inga’s identity is authenticated **302** by an authentication module using the authentication credentials that the user **110**, Inga, input into the system. In this example, Inga’s identity is authenticated and she is assigned a role (Role AssignmentID=“E1”), which, for this example, is the role of “CSS Rep.” Based on the Role AssignmentID of “E1,” context parameters are obtained **303**. For this example, organizational context parameters (OrgContext ContextID=“C”) are passed back, including the “DC” practice context parameter, and the “ECM” market segment

context parameter. In this example, no specific values for the client context parameter and the plan context parameter are set. In this example, the client and plan context parameters can be variable. One or more policy instances, for this example, can be resolved based upon the context parameters requested by the consuming application. For this example, as part of the “resolve role” process **304**, a actor-role scope key or pointer value of “FPRS” is set so that the scope for Inga’s role can be resolved.

```

<GetRoles>
  <Identity>Inga</Identity>
</GetRoles>
<GetRolesResponse>
  <Identity>Inga</Identity>
  <Roles>
    <Role AssignmentID="E1">
      <RoleName>CSS Rep</RoleName>
      <OrgContext ContextID="C">
        <Practice value="DC">
          <MarketSegment value="ECM">
            <Client value="*">
              <Plan value="*">
                </Client>
              </MarketSegment>
            </Practice>
          </OrgContext>
          <ScopeQualifier>
            <ScopeResolver>FPRS</ScopeResolver>
            <Qualifier>
              <Practice value="DC"/>
              <MarketSegment value="ECM"/>
              <Client value="All except XYZ"/>
              <Plan value="All except XYZ plans"/>
              <Division value="All except XYZ executives"/>
            </Qualifier>
          </ScopeQualifier>
        </Role>
      </Roles>
    </GetRolesResponse>
  
```

[0055] In this example, session context parameters are retrieved, including the “BWS” application value context parameter, the “PSG” point of claim context parameter, and the authentication credential strength context parameter of “5.” In this example, based on the role of the user **110**, “Inga,” the session context parameters, e.g., “BWS,” “PSG,” and “5,” and the organizational context parameters associated with OrgContext ContextID “C,” one or more policy instances are retrieved. In this example, policy instances are retrieved that include, instances of the policy type “performance management” (PolicyInstance InstanceID “15”), policy type “timekeeping functions” (PolicyInstance InstanceID “16”), and policy type “DC transactions” (PolicyInstance InstanceID “19”). Each of the unique policy instances for this example, contain a set of policy elements with values that can aid in the determination of user access authorizations. For example, according to PolicyInstance InstanceID “16,” which includes a policy element “enter timekeeping data” that is set to “N,” the user **110**, “Inga,” cannot enter timekeeping data given that she is an independent contractor.

```

<GetPolicySet>
  <RoleAssignmentID>E1/RoleAssignmentID>
  <Context>
  
```