

21

authorizing a requesting entity to operate upon data structures in a standard manner, the method comprising:

an act of maintaining a number of role templates within a plurality of role map documents that are each specific to a computerized service that is configured to perform computerized operations on data structures, the role templates defining basic access permissions with respect to a number of command methods, wherein at least some of the role templates define the basic access permissions in a manner that is independent of the type of data structure being operated upon; and

a step for authorizing a requesting entity using the role templates in a manner that is independent of the type of data structure being accessed.

30. A method in accordance with claim **29**, wherein the step for authorizing a requesting entity using the role templates comprises the following:

an act of maintaining a plurality of role definitions that define access permissions for receiving entities by using one or more of the role templates;

an act of receiving a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity as well as an application-platform identifier corresponding to an application of the computerized service;

an act of identifying a role definition corresponding to the requesting entity; and

an act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity.

31. A method as recited in claim **29**, wherein the act and step are performed by a processor executing computer-executable instructions embodied within a physical computer-readable medium.

32. A computer program product for use in a computer network that includes different types of data structures of one or more specific entities, the computer program product for implementing a method for authorizing a requesting entity to operate upon data structures in a standard manner, the computer program product comprising one or more computer-readable storage media have stored thereon the following:

computer-executable instructions for maintaining a plurality of role templates that define basic access permissions with respect to one or more command methods, wherein at least some of the role templates define the basic access permissions in a manner that is independent of the type of data structure being operated upon, and wherein the plurality of role templates are contained within a plurality of role map documents, each role map document being specific to a particular computerized service that is configured to perform computerized operations on data structures;

computer-executable instructions for maintaining a plurality of role definitions that define access permissions for receiving entities by using one or more of the role templates;

computer-executable instructions for detecting the receipt of a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity as well as an application-platform identifier corresponding to an application of the computerized service;

computer-executable instructions for identifying a role definition corresponding to the requesting entity; and

22

computer-executable instructions for determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity.

33. In a computer network that includes different services, applications, and an authorization station, the applications submitting requests to perform operations on different data structures managed by the different services, a system for isolating the authorization process from the services so that the services need not independently authorize each request they receive from the number of applications, the system comprising:

a plurality of computerized services that are configured to perform computerized operations on data structures;

an authorization station configured to receive requests from a number of applications to operate upon data structures managed by any of the number of services, the authorization station configured to perform the following:

receive a request from a requesting entity to perform a target operation upon a target data structure managed by a target service, wherein the request includes an application-platform identifier corresponding to an application of the computerized service;

access a role template that defines basic authorizations with respect to one or more operations, including at least the target operation, wherein the role template defines the basic authorizations in a manner that is independent of the target data structure desired to be operated upon, and wherein the role template is contained within a role map document that is specific to one of the plurality of services and accessed from among a plurality of role map documents each specific to one of the plurality of services;

determine that the corresponding requesting entity is authorized to perform the target operation on the target data structure; and

communicate to the target service that the requesting entity is authorized to perform the target operation on the target data structure.

34. A method as recited in claim **1**, wherein the act of maintaining a plurality of role definitions that define access permissions for requesting entities by using one or more of the role templates comprises the following:

an act of maintaining a plurality of role definitions for the requesting entity, wherein at least one of the plurality of role definitions corresponds to an authentication method.

35. A method as recited in claim **1**, wherein the act of identifying a role definition corresponding to the requesting entity comprises the following:

an act of referencing a role template; and

an act of maintaining one or more refined scopes for refining a scope referenced in the role template, wherein the one or more refined scopes are independent of the role template and refinement occurs at a user level, and wherein the scope referenced in the role template indicates what portions of a data structure are visible to a role definition for a particular command method.

36. A method as recited in claim **1**, wherein the act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting comprises the following: