CLAIMS

What is claimed is:

1. A method in a computing system, supporting a plurality of tenants accessing genomic digital data resources provided by one or more genomic data services in a software-as-a-service platform that orchestrates access to the genomic digital data resources via policy-based access control, the method comprising:

receiving a policy-based access control definition for a first of the tenants for a given genomic digital data resource, wherein the genomic digital data resource comprises genomic data originating from a sequencing instrument, and the policy-based access control definition supports access control statements that specify one or more conditions under which access is granted;

receiving a request for access to the given genomic digital data resource from a second of the tenants seeking access to the given genomic digital data resource, wherein the request comprises one or more attributes;

accessing the policy-based access control definition responsive to the request from the second of the tenants;

generating an access token based on the one or more attributes and the one or more conditions;

adding a role identifier of the policy-based access control definition into the access token; and

granting the second tenant access to the given genomic digital data resource based on the policy-based access control definition.

2. The method of claim 1 wherein:

access to the given genomic digital data resource is controlled by a role identifier linked to the policy-based access control definition; and

the method further comprises:

responsive to the request for access, providing the role identifier specified in the policy-based access control definition for the request for access.

3. The method of claim 2 wherein:

assigning the role identifier comprises late binding of the role identifier to a user identifier or tenant identifier of the request for access.

4. The method of any one of claims 2-3 further comprising:

responsive to the request for access, generating a signed access token containing the role identifier;

wherein access is granted based on presence of the role identifier in the signed access token.

5. The method of claim 4 further comprising:

publishing a signed grant token comprising the role identifier and a tenant identifier of a role administrator of the role identifier;

wherein access is further granted based on whether the tenant identifier of the signed grant token has sufficient rights to grant resources specified for the role identifier.

6. The method of any one of claims 1-5, wherein the first of the tenants comprises a proxy tenant representing an external service provider for which policy-based sharing is implemented.

7. The method of any one of claims 1-6 wherein the policy-based access control definition specifies one or more access control statements comprising a filter attribute and a filter parameter.

8. The method of claim 7 wherein the filter parameter specifies a wildcard for the filter attribute.

9. The method of any one of claims 7-8 wherein the filter attribute comprises an application.

10. The method of any one of claims 7-9 wherein the filter attribute comprises an application role identifier.

11. The method of any one of claims 1-10 wherein the policy-based access control definition comprises a parameter evaluated at execution time.

12. The method of claim 11 wherein:

the parameter of the policy-based access control definition comprises an application identifier parameter; and

granting access comprises comparing the application identifier parameter of the policy-based access control definition with an application identifier specified by the second of the tenants seeking access to the genomic digital data resources.

13. The method of any one of claims 11-12 wherein:

the parameter of the policy-based access control definition comprises a tenant identifier parameter; and

granting access comprises comparing the tenant identifier parameter of the access control definition with a tenant identifier of the second tenant seeking access to the genomic digital data resources.

14. One or more computer-readable media comprising computer-executable instructions that when executed by a computing system, cause the computing system to perform the method of any one of claims 1-13.

15. A multi-tenant, cloud-based system comprising:

one or more processors;

memory coupled to the one or more processors;

a policy store comprising a policy-based access control definition received for a first tenant, a role identifier and one or more conditions;

a genomic digital data resource linked to the role identifier, wherein the genomic digital data resource comprises genomic data originating from a sequencing instrument;

wherein the memory comprises computer-executable instructions causing the one or more processors to perform operations comprising:

receiving a request for access to the genomic digital data resource from a second tenant seeking access to the genomic digital data resource, wherein the request comprises one or more attributes;

accessing the policy-based control definition responsive to the request from the second tenant for access;

generating an access token based on the one or more attributes and the one or more conditions;

adding the role identifier into the access token responsive to determining that the one or more conditions are fulfilled by the one or more attributes; and

granting the second tenant access to the genomic digital data resource according to the policy-based access control definition evaluated at a time of the request for access.