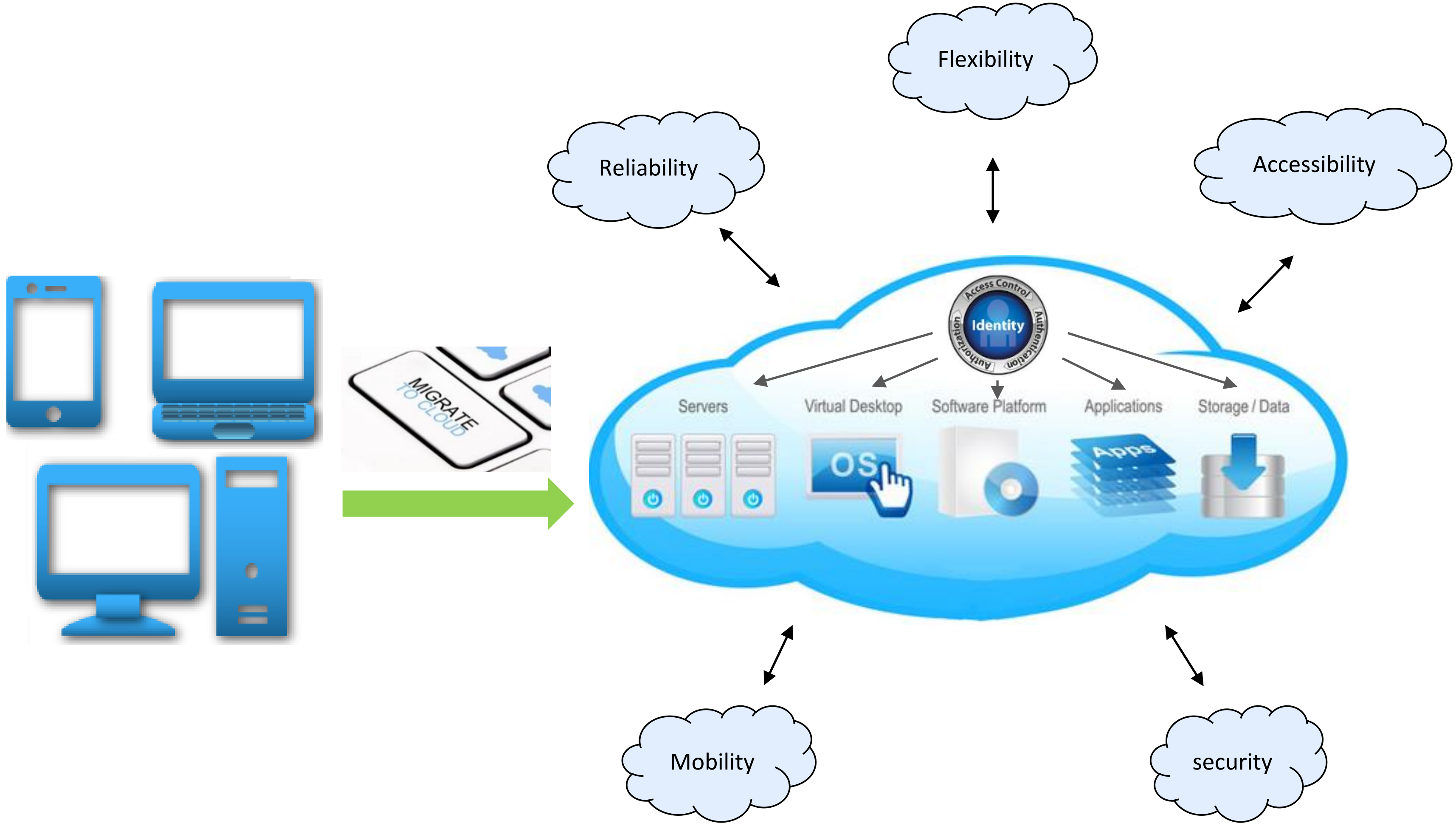
Authorization Federation in Multi-Tenant Multi-Cloud IaaS

Navid Pustchi

Advisor: Prof. Ravi Sandhu

“Moving” to Cloud



Flexibility

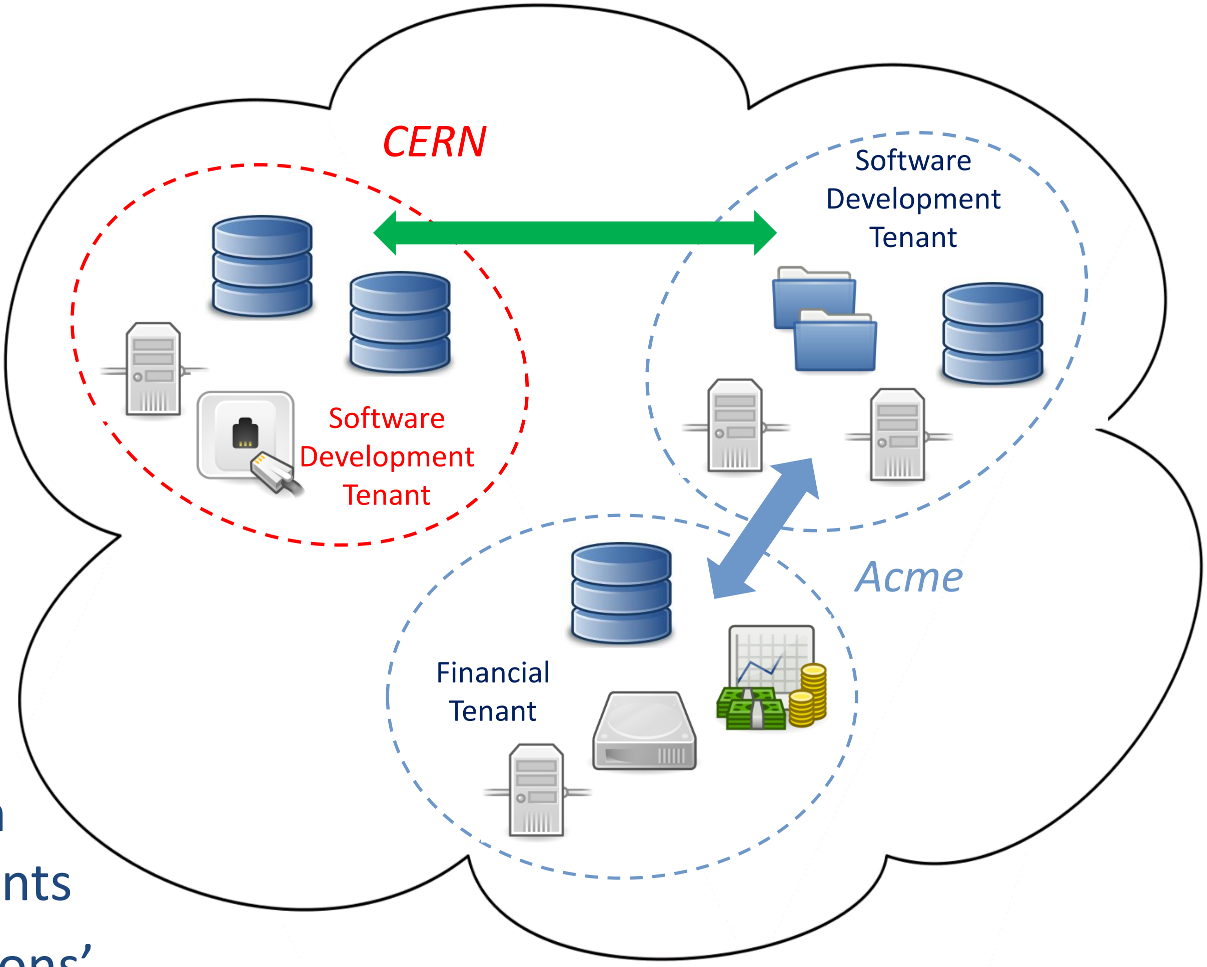
Reliability

Accessibility

Mobility

security

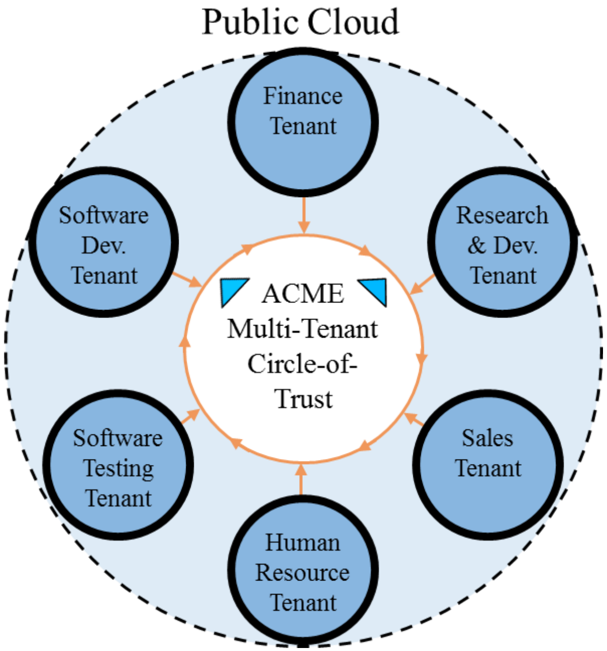
Why Collaboration ?

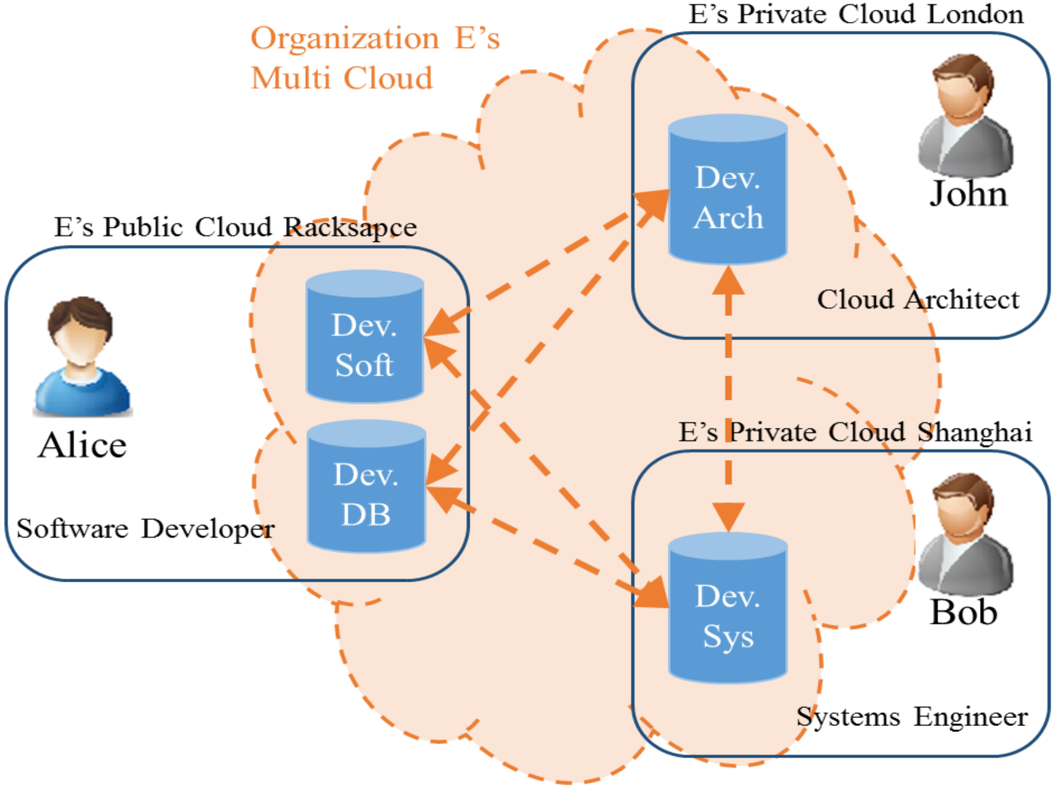


- Large Organization with multiple tenants
- Distinct Organizations' Collaborative tasks

Cloud Service Provider

Why Multi Cloud?



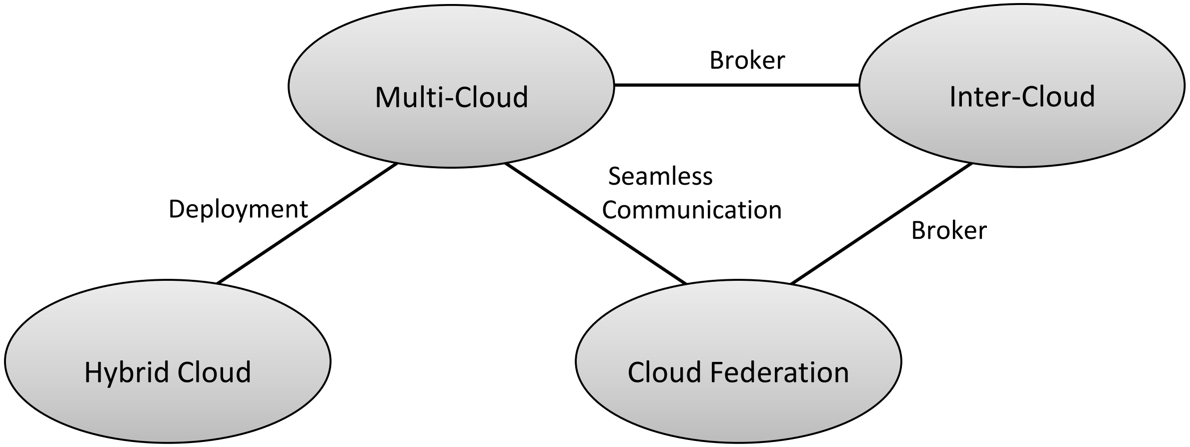


World-Leading Research with Real-World Impact!

Federation

- Cloud Federation
  - Collaboration of cloud service providers and identity providers in order to share their services and resources based on trust agreements.

- Multi-Cloud
  - Collaboration of multiple cloud service providers (public or private) within different administrative domains (Cloud and Domain) to provide complex services at specified service model (Infrastructure, Platform and Software).



Multi Cloud Collaboration

- Cloud Federation
  - Service (IaaS, PaaS, SaaS)
    - Heterogeneous: Google account (Open ID 2.0) Heterogeneous within google.
    - Homogeneous: Eduroam federated network access.
  - Platform
    - Heterogeneous: OpenStack federation with AWS.
    - Homogeneous: Keystone to Keystone federation.
  - Trust
    - Circle-of-Trust: Alliance of institutions for sharing scientific data such as CERN.
    - Peer-to-Peer: Best Buy federating with Rackspace.
  - Coupling
    - Identity Federation: SAML, OAuth, OpenID, SSO.
    - Authorization Federation: SAML, OAuth.

Problem & Thesis

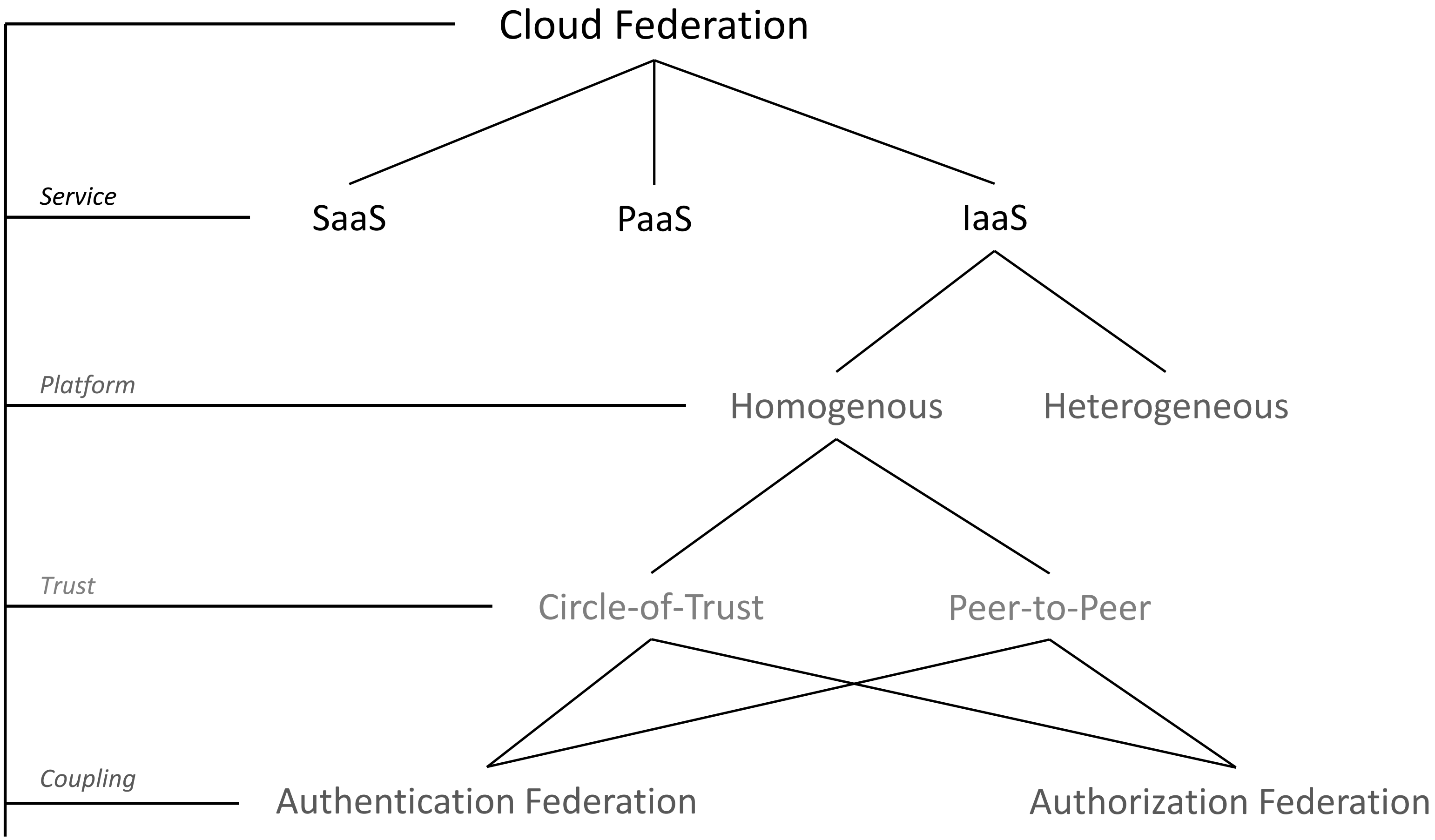
- Problem Statement

Current access control models provided by cloud platforms are not sufficient to cultivate efficient peer-to-peer and circle-of-trust collaboration between tenants in a cloud or across multiple cloud platforms. Prior role-based and attribute-based access control models in distributed systems are not effectively applicable to cloud IaaS.

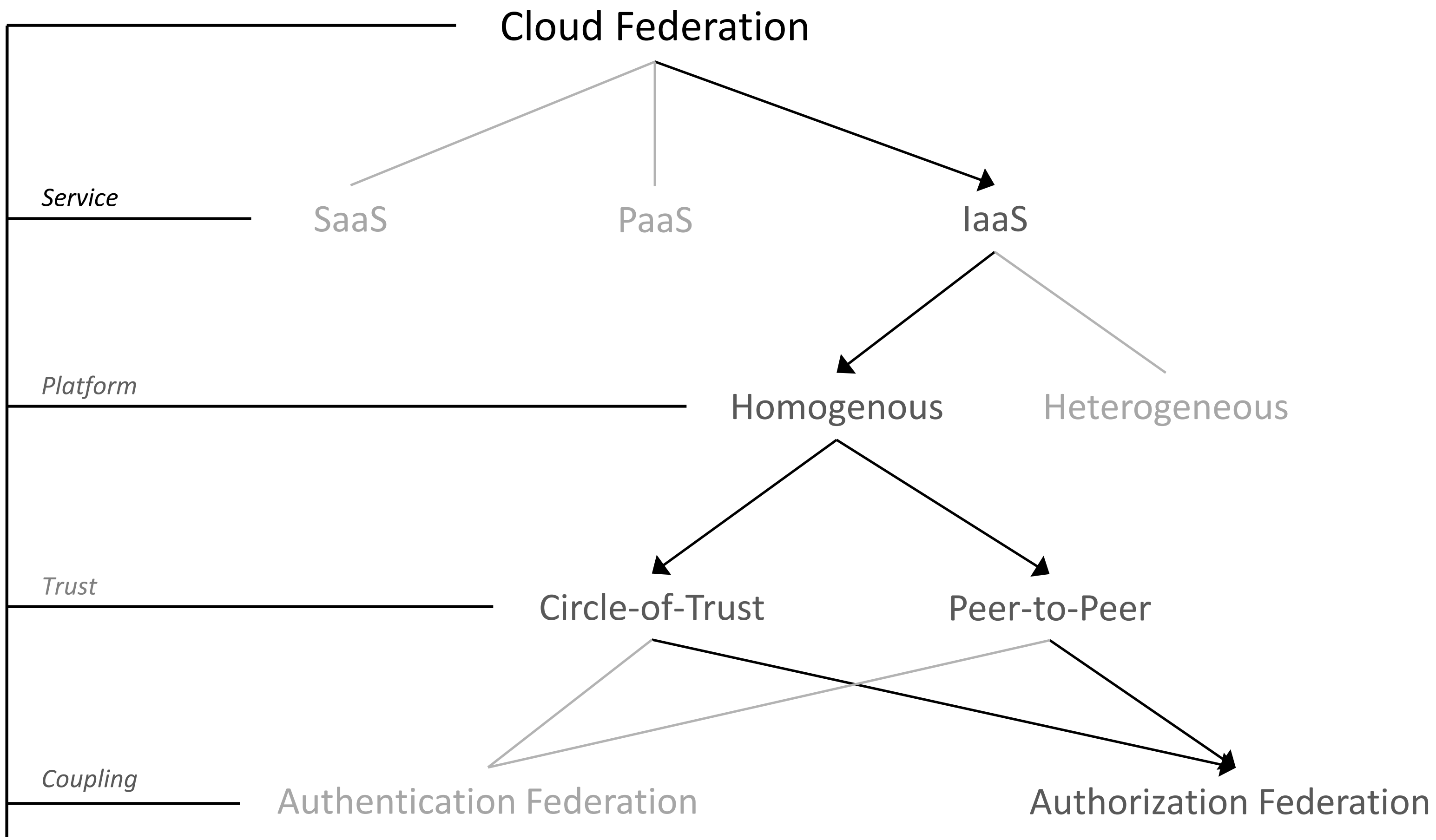
- Thesis Statement

The problem of authorization federation in multi-tenant cloud IaaS can be partially solved by integrating multiple types of peer-to-peer and circle-of-trust relations between tenants in single-cloud and multi-cloud environments into role-based and attribute based models.

Scope of Contribution



Scope of Contribution

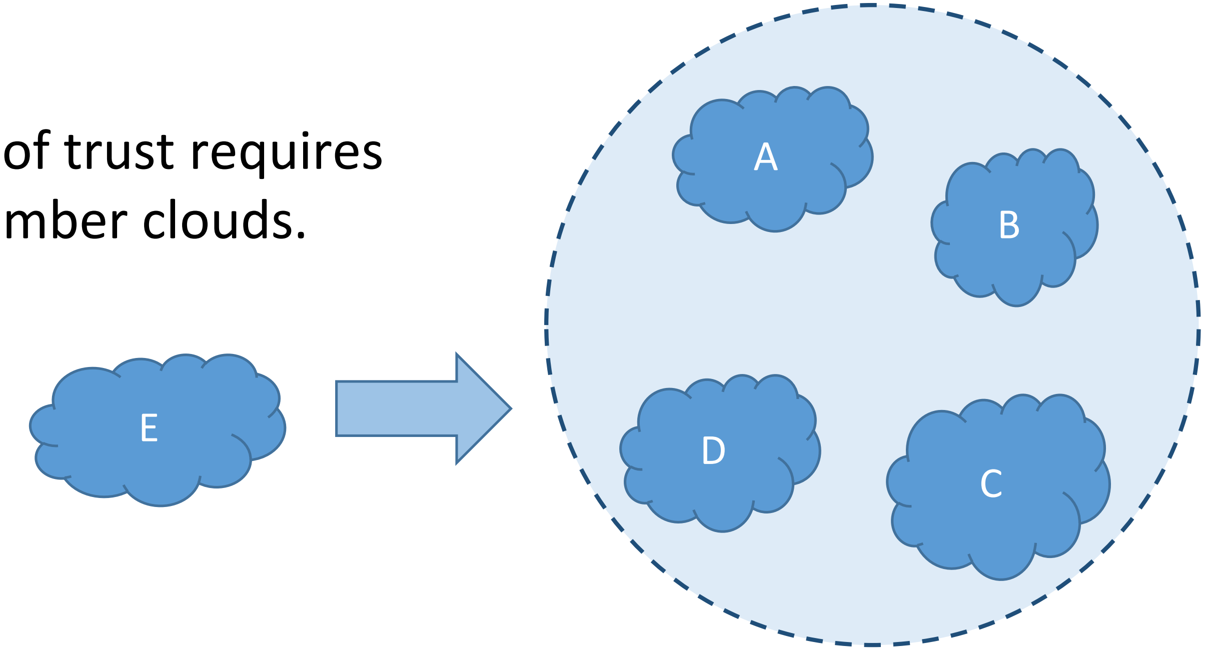


Circle-of-Trust

- A collaboration group of clouds, relationships are established by a set of contracts defining obligations and access rights of participating clouds.

- Member clouds have access to a set of shared services and resources.

- Joining the circle of trust requires agreement of member clouds.

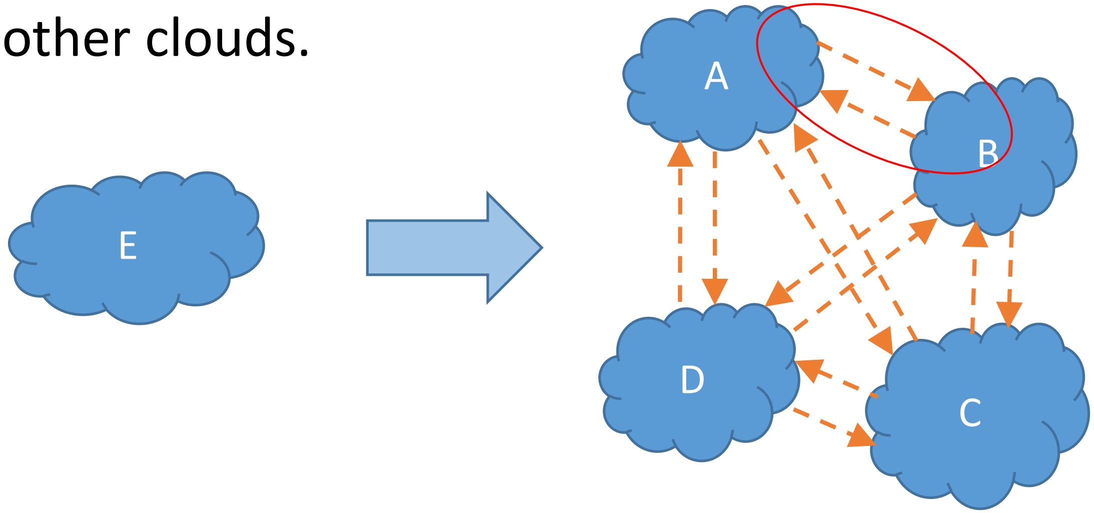


Peer-to-Peer Trust

- Collaboration of clouds, relationships established between each two participating clouds.

- Clouds share resources and services upon trust relationship between trustor and trustee clouds.

- Joining a new relationship requires stablishing trust with other clouds.

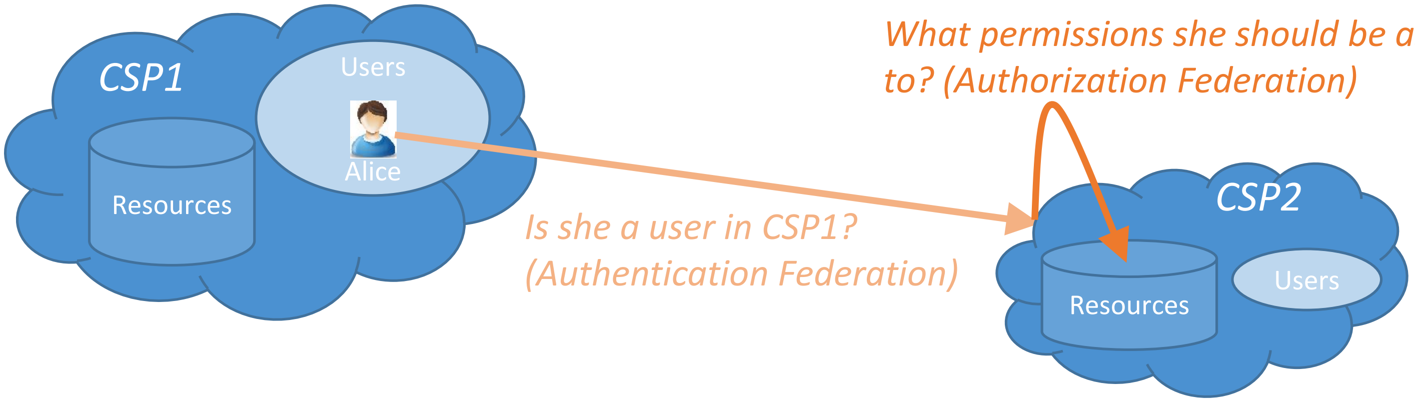


Identity vs Authorization

- Identity (Authentication) Federation:
  - Authenticating users (services and applications) in a cloud service provider other than their registered identity provider based on trust between collaborating clouds.

- Authorization Federation:
  - Granting access to authenticated users by assigning roles in cloud service provider based on trust agreements between two clouds.

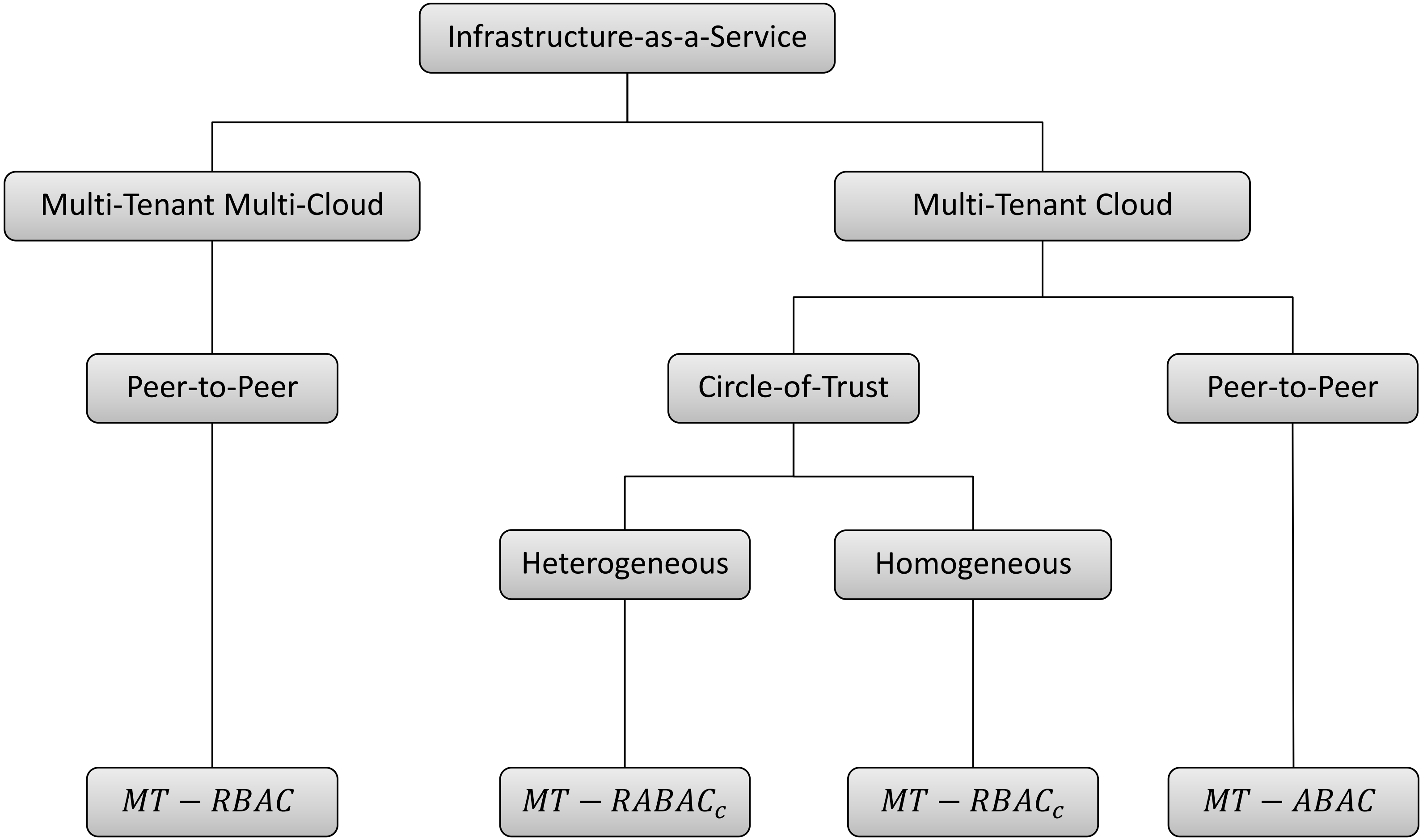
- Authorization federation is dependent on identity federation to authenticate users.



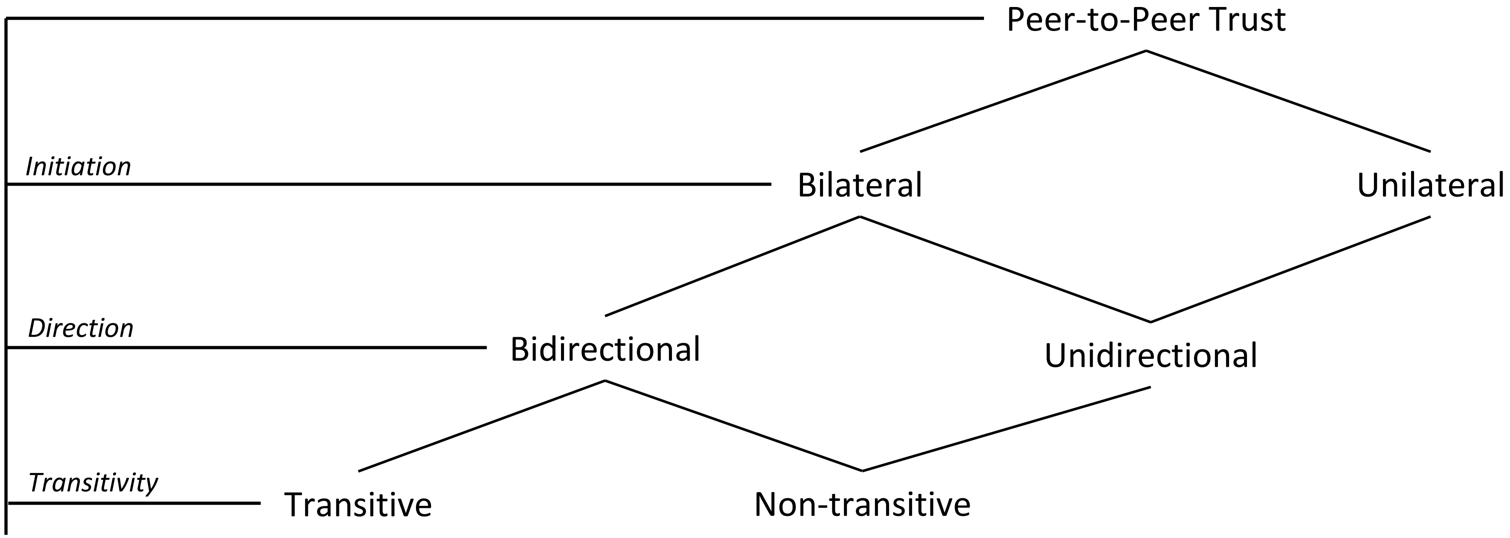
What permissions she should be assigned to? (Authorization Federation)

Is she a user in CSP1? (Authentication Federation)

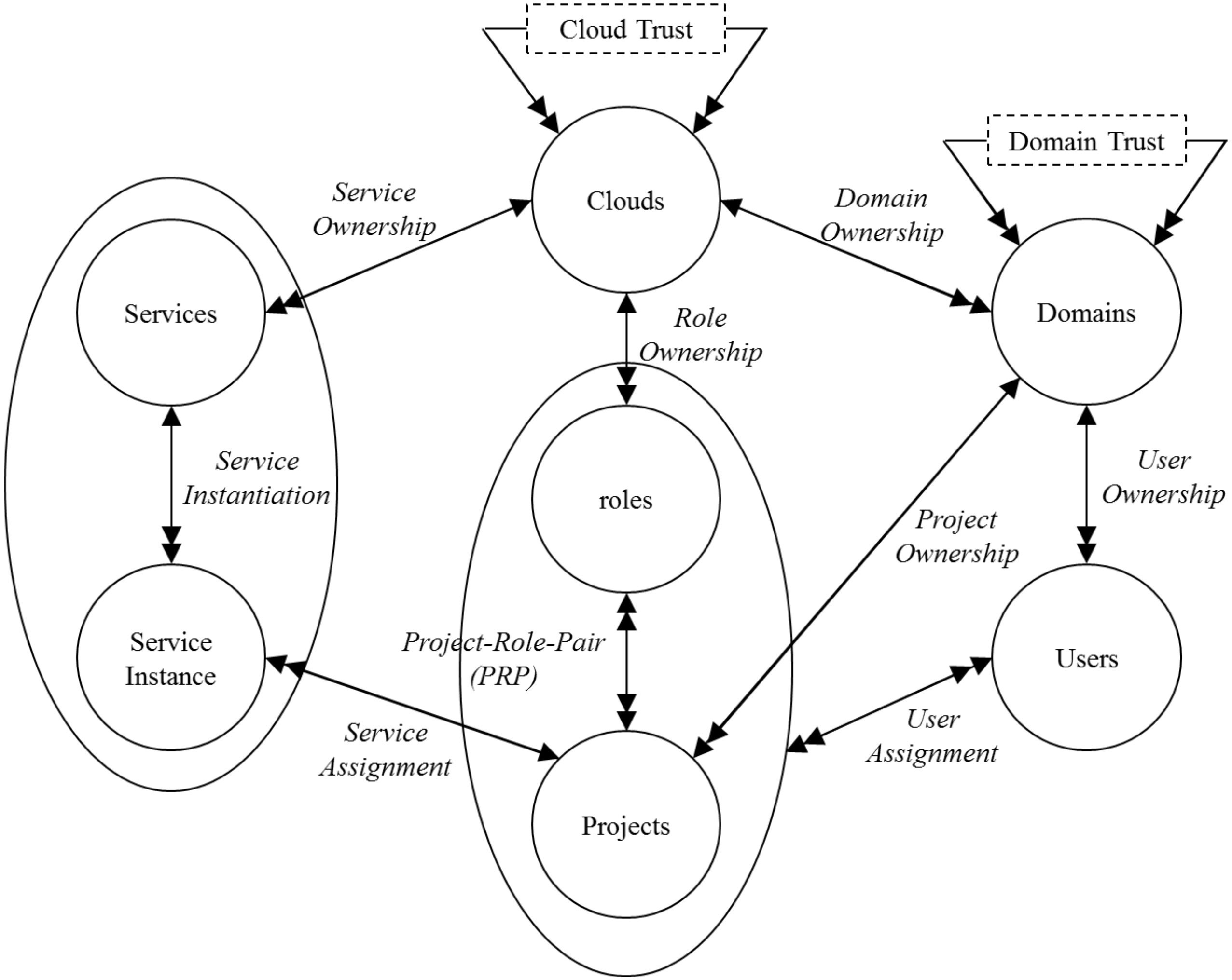
Contribution



Peer-to-Peer Trust



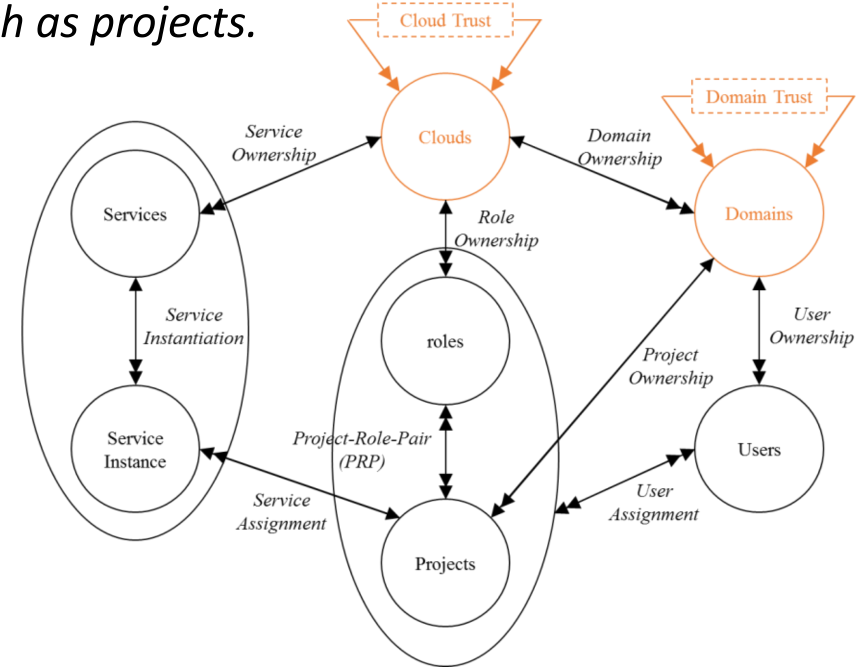
Administrative Realms



World-Leading Research with Real-World Impact!

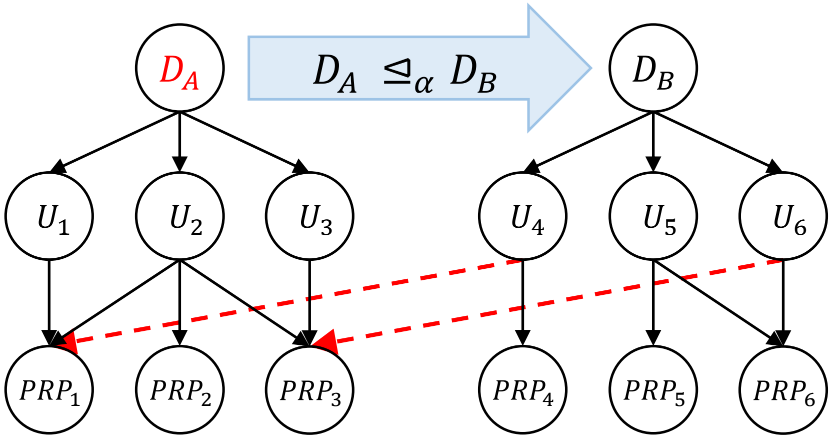
Multi Cloud Trust

- Two trust scopes based on administrative realms in cloud:
  - *Cross Cloud Trust*
    - *Sharing cloud infrastructure resources, such as services.*
  - *Cross Domain Trust*
    - *Sharing domain resources such as projects.*



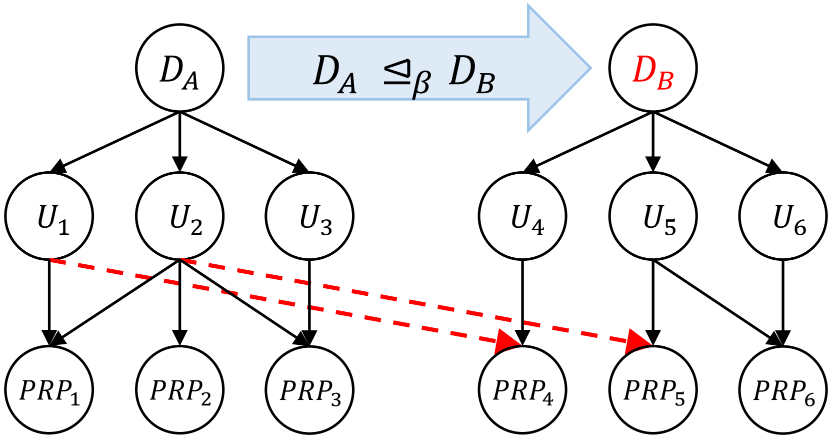
Domain Trust

- $\boldsymbol{Type - \alpha}$:
  - *If* $domain_A \trianglelefteq_\alpha domain_B$, *A is authorized to assign B's users to it's resources. A controls trust relation and inter-cloud assignments.*
  - For example cloud B act as an identity provider to access A's resources.



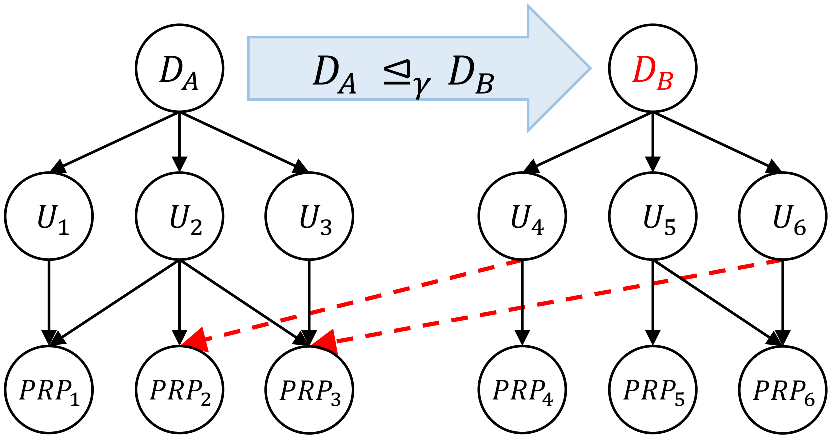
Domain Trust

- **$Type - \beta$**:
  - *If $domain_A \trianglelefteq_\beta domain_B$, B is authorized to assign A's users to it's resources. A controls trust relation and B controls inter-cloud assignments.*
  - When access to shared resources is controlled by resource owner.



Domain Trust

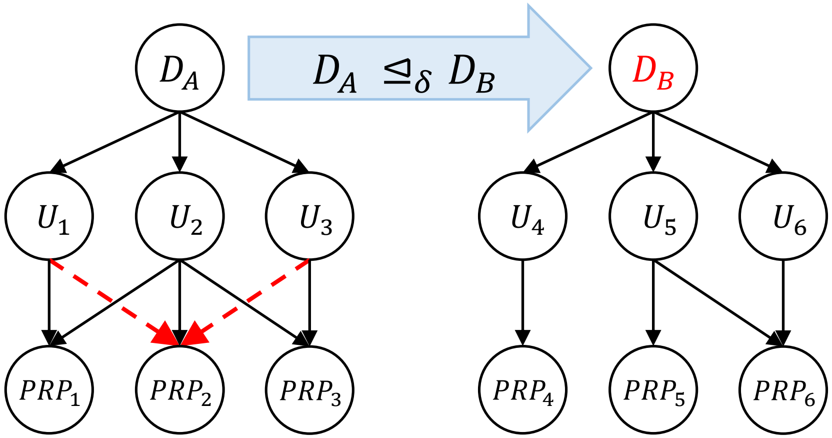
- $\boldsymbol{Type - \gamma}$:
  - *If* $domain_A \trianglelefteq_\gamma domain_B$, *$B$ is authorized to assign it's users to A's resources. A controls trust relation and B controls inter-cloud assignments.*
  - Sharing resources with group of clouds.



World-Leading Research with Real-World Impact!

Domain Trust

- $\boldsymbol{Type - \delta}$:
  - *If* $domain_A \trianglelefteq_\delta domain_B$*,* B *is authorized to assign* A*'s users to* A*'s resources.* A *controls trust relation and* B *controls intra-cloud assignments*.
  - Administration federation within an organization with multiple clouds.



World-Leading Research with Real-World Impact!

Attribute Based Access Control (ABAC)

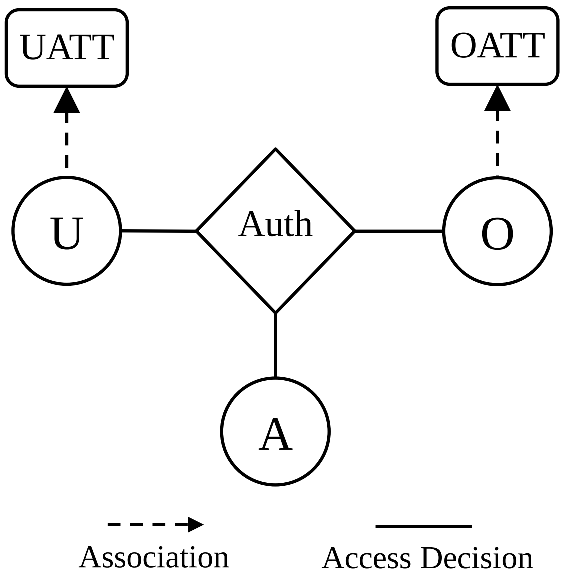
- Attributes are *name:value* pairs
  - Represents user and resource properties
- Associated with
  - Users
  - Objects
  - Tenants
  - Contexts
- Converted to rights by authorization policies
  - In-time
  - Entity attributes
  - Set of actions

Why Another Model

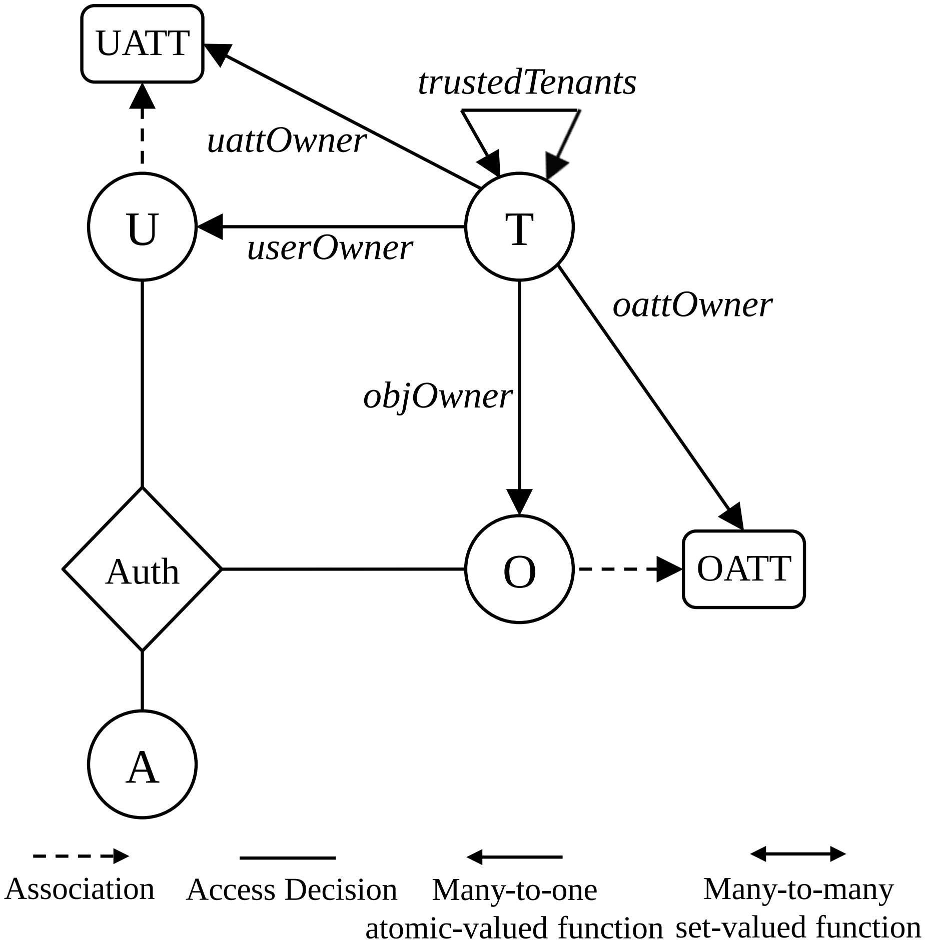
- ABAC
  - RBAC shortcomings needs custom extension
    - For example real time environmental parameters.
  - ABAC is more flexible
    - Accommodate environmental parameters.

- MT-ABAC
  - Multi-tenancy
  - Collaboration consistent with trust

$ABAC_0$ Model Structure

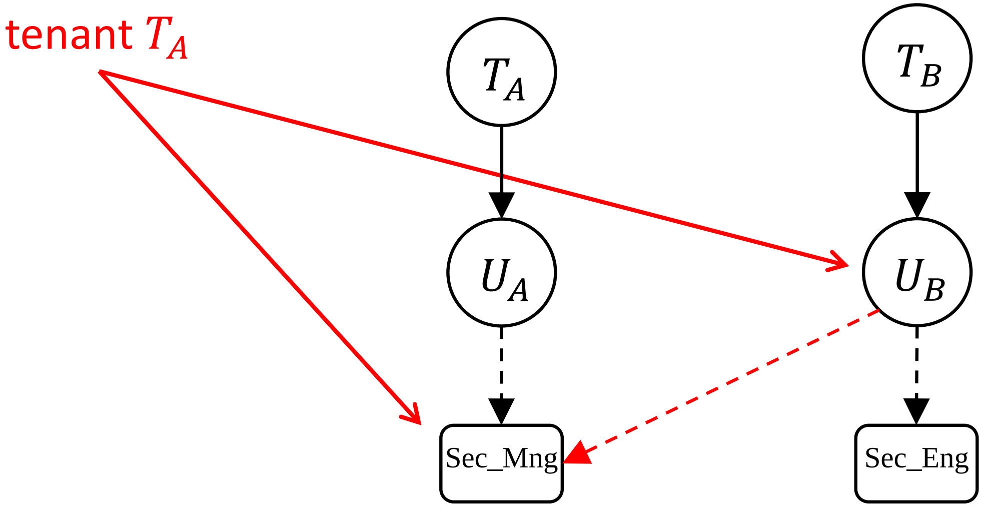


$MT - ABAC_0$ Model Structure



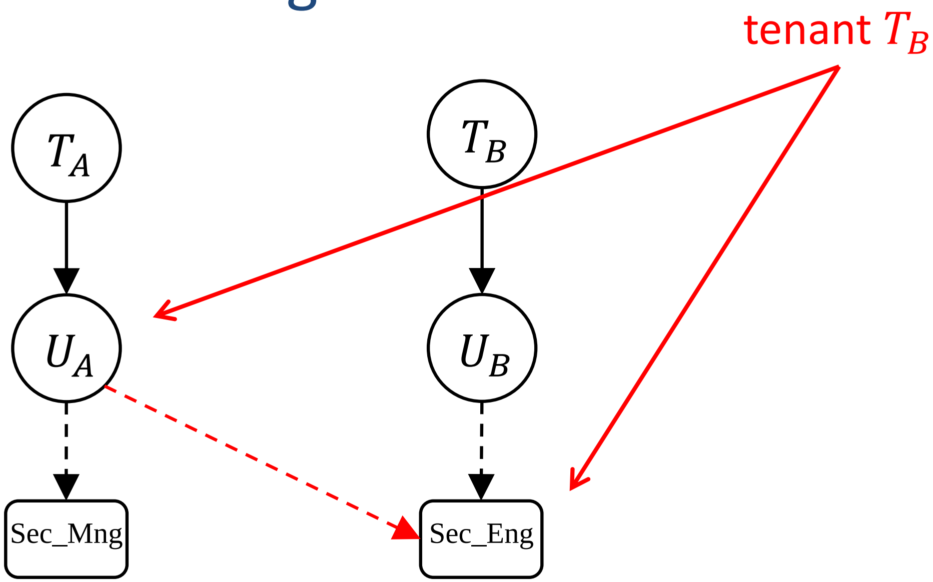
Tenant-Trust

- Tenant-trust type-α
  - If $T_A \trianglelefteq_\alpha T_B$, tenant T_A is authorized to assign values for T_A's user attributes to tenant T_B's users. Tenant $T_A$controls tenant-trust existence and cross-tenant attribute assignments.



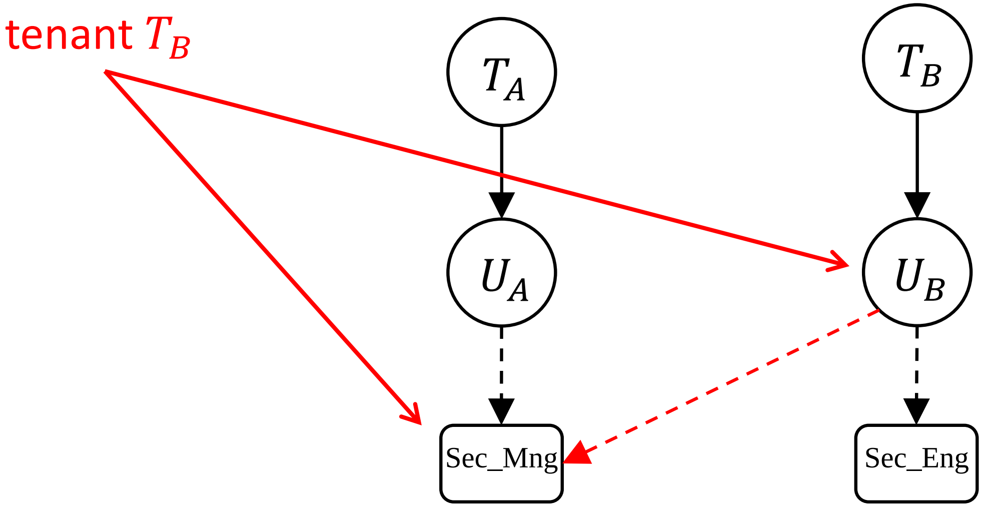
Tenant-Trust

- Tenant-trust type-β
  - If $T_A \trianglelefteq_\beta T_B$, tenant T_B is authorized to assign values for T_B's user attributes to tenant T_A's users. Tenant $T_A$controls tenant-trust existence while T_B controls cross-tenant attribute assignments.

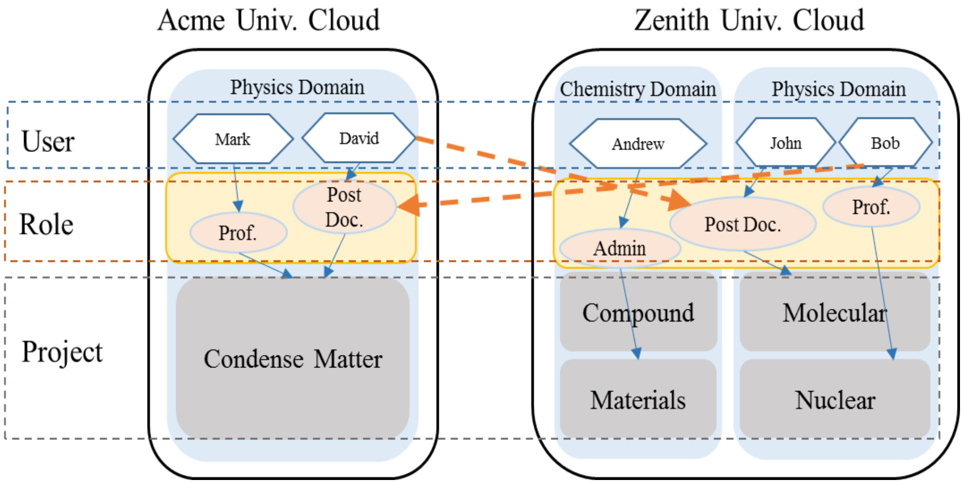


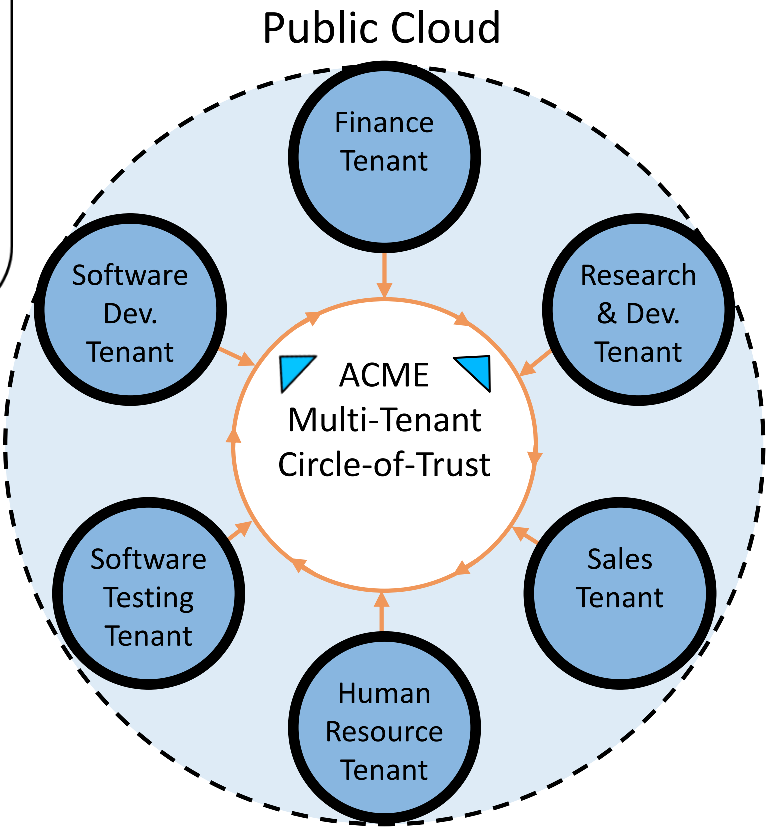
Tenant-Trust

- Tenant-trust type-γ
  - If $T_A \trianglelefteq_\gamma T_B$, tenant T_B is authorized to assign values for T_A's user attributes to tenant T_B's users. Tenant $T_A$controls tenant-trust existence while T_B controls cross-tenant attribute assignments.

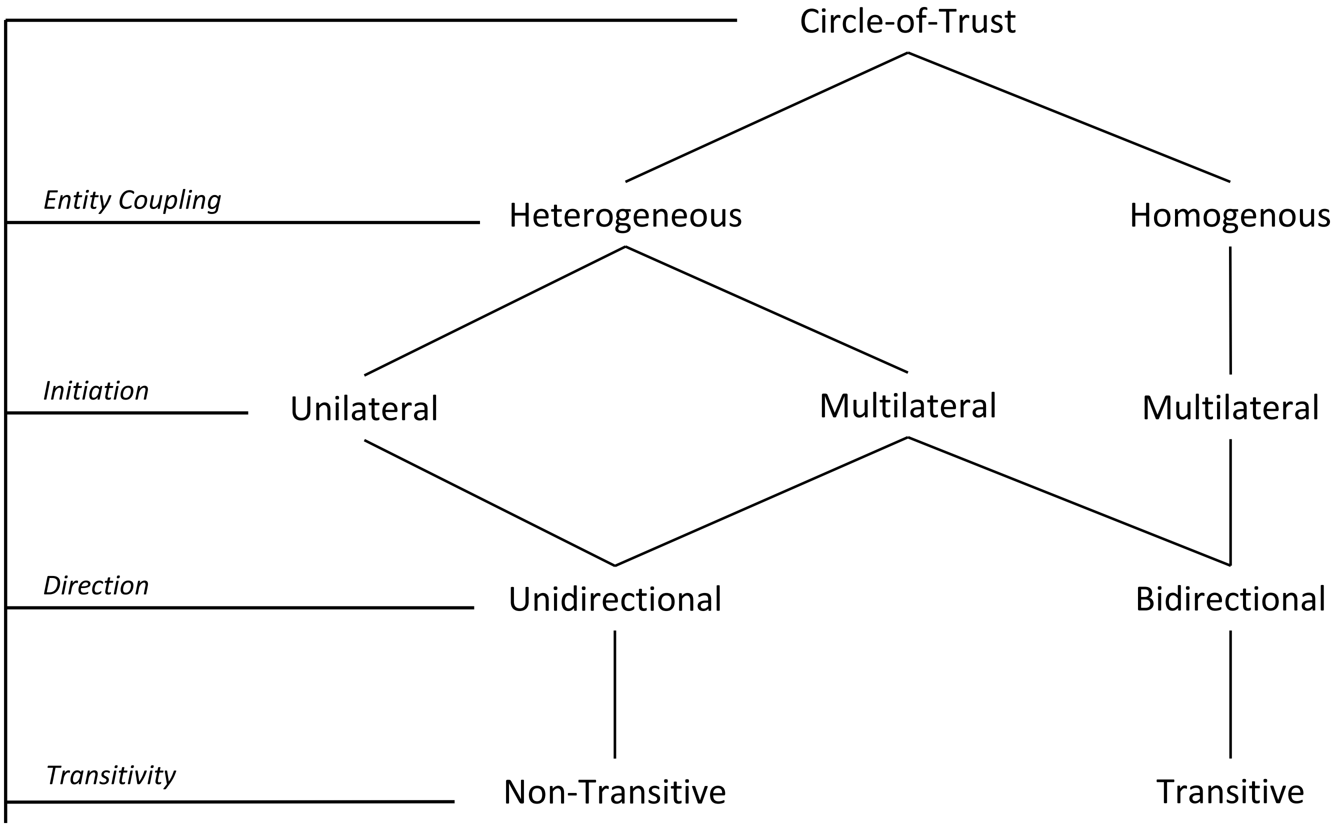


P2P vs. CoT


Acme Univ. Cloud
Zenith Univ. Cloud
Physics Domain
Chemistry Domain
Physics Domain
User
Role
Project
Mark
David
Andrew
John
Bob
Post Doc.
Prof.
Admin
Post Doc.
Prof.
Condense Matter
Compound
Molecular
Materials
Nuclear

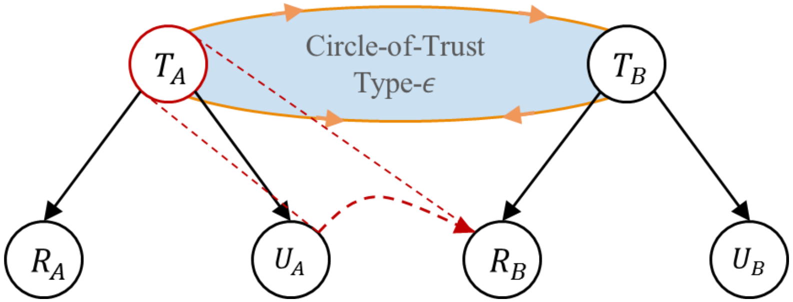

Public Cloud
Finance Tenant
Software Dev. Tenant
Research & Dev. Tenant
ACME Multi-Tenant Circle-of-Trust
Software Testing Tenant
Sales Tenant
Human Resource Tenant

Trust in Circle-of-trust

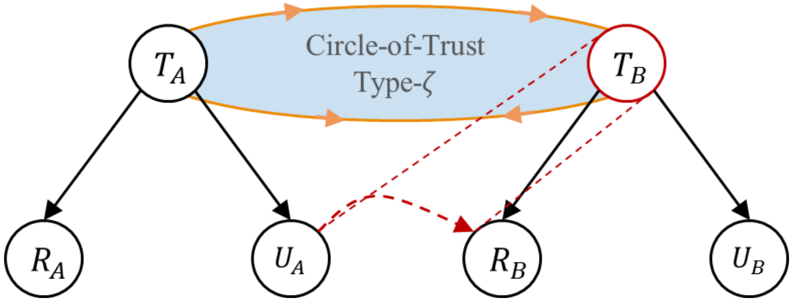


Tenant-Trust in CoT

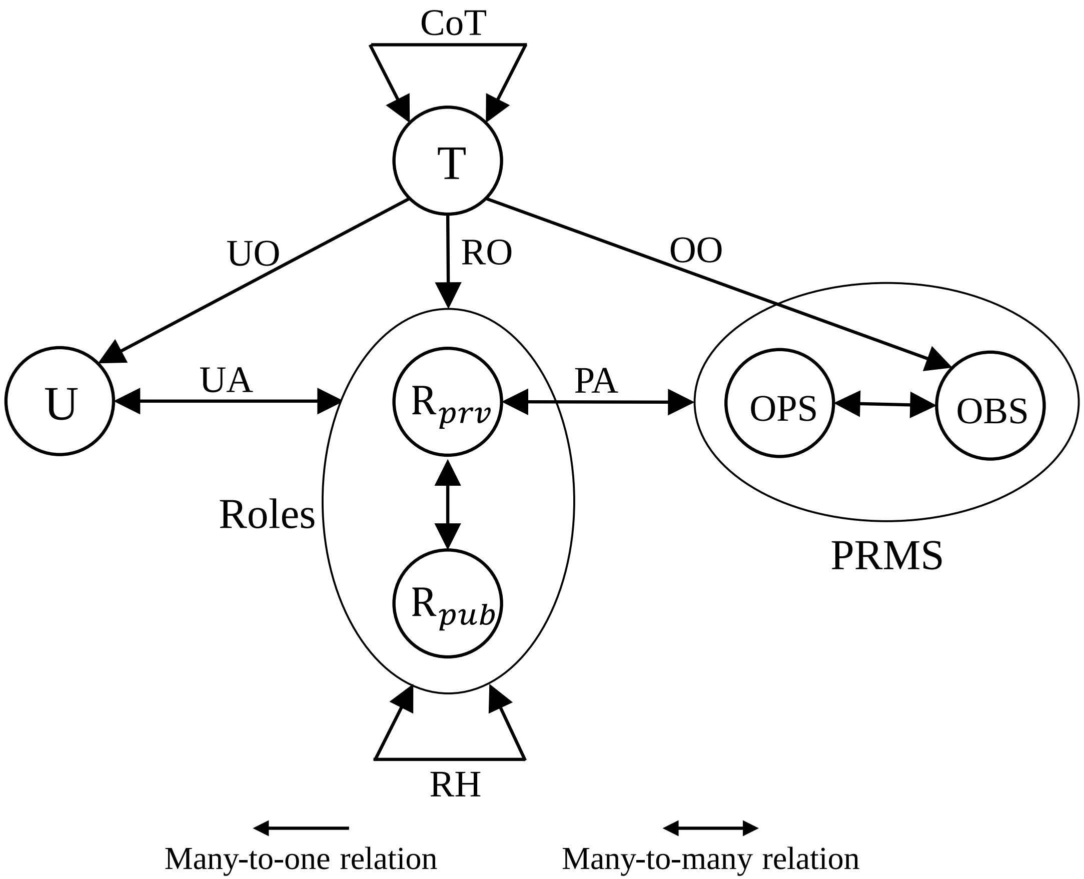
- Four trust types:
  - $\boldsymbol{Type-\varepsilon}$:
    - *If $T_A \trianglelefteq_\varepsilon T_B$, then tenant T_A is authorized to assign its users to T_B's roles. Tenant T_A controls user assignments.*



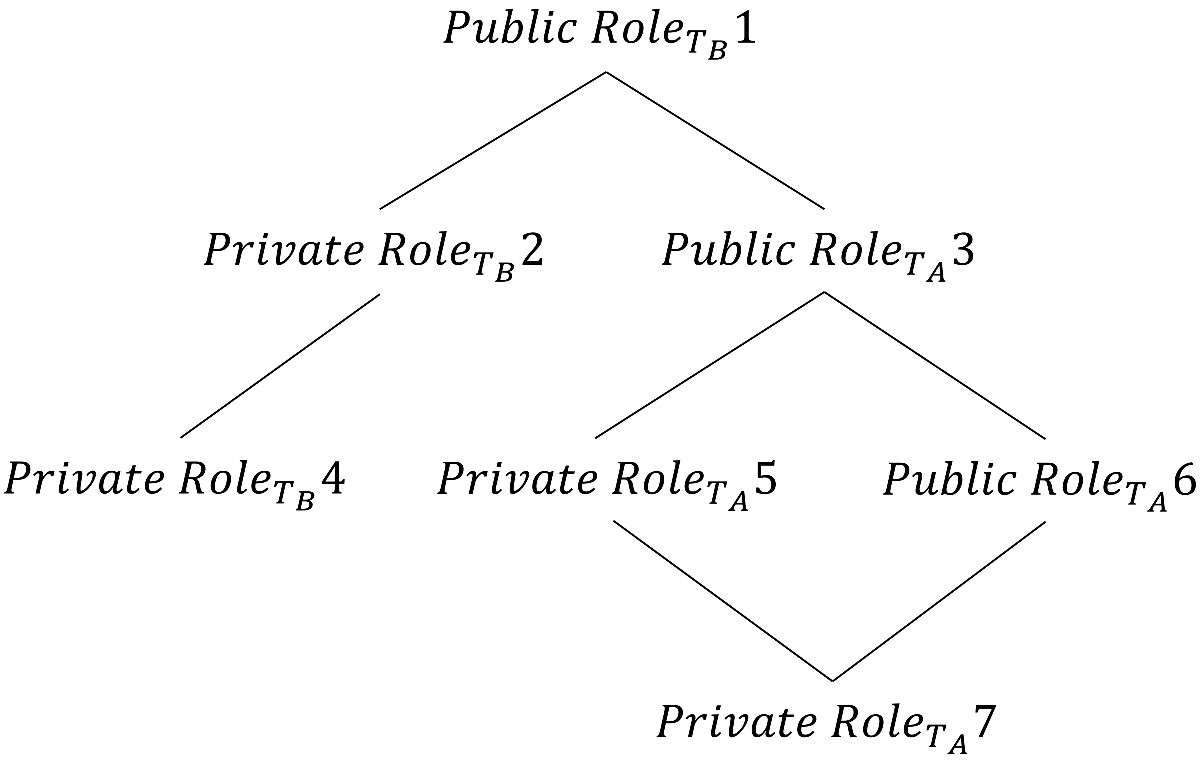
  - $\boldsymbol{Type-\zeta}$:
    - *If $T_A \trianglelefteq_\zeta T_B$, then tenant T_B is authorized to assign T_A's users to its roles. Tenant T_B controls user assignments.*



$MT - RBAC_c$


CoT
T
UO
RO
OO
U
UA
R_{prv}
PA
OPS
OBS
Roles
PRMS
R_{pub}
RH
Many-to-one relation
Many-to-many relation

$MT-RBAC_c$ Role Hierarchy



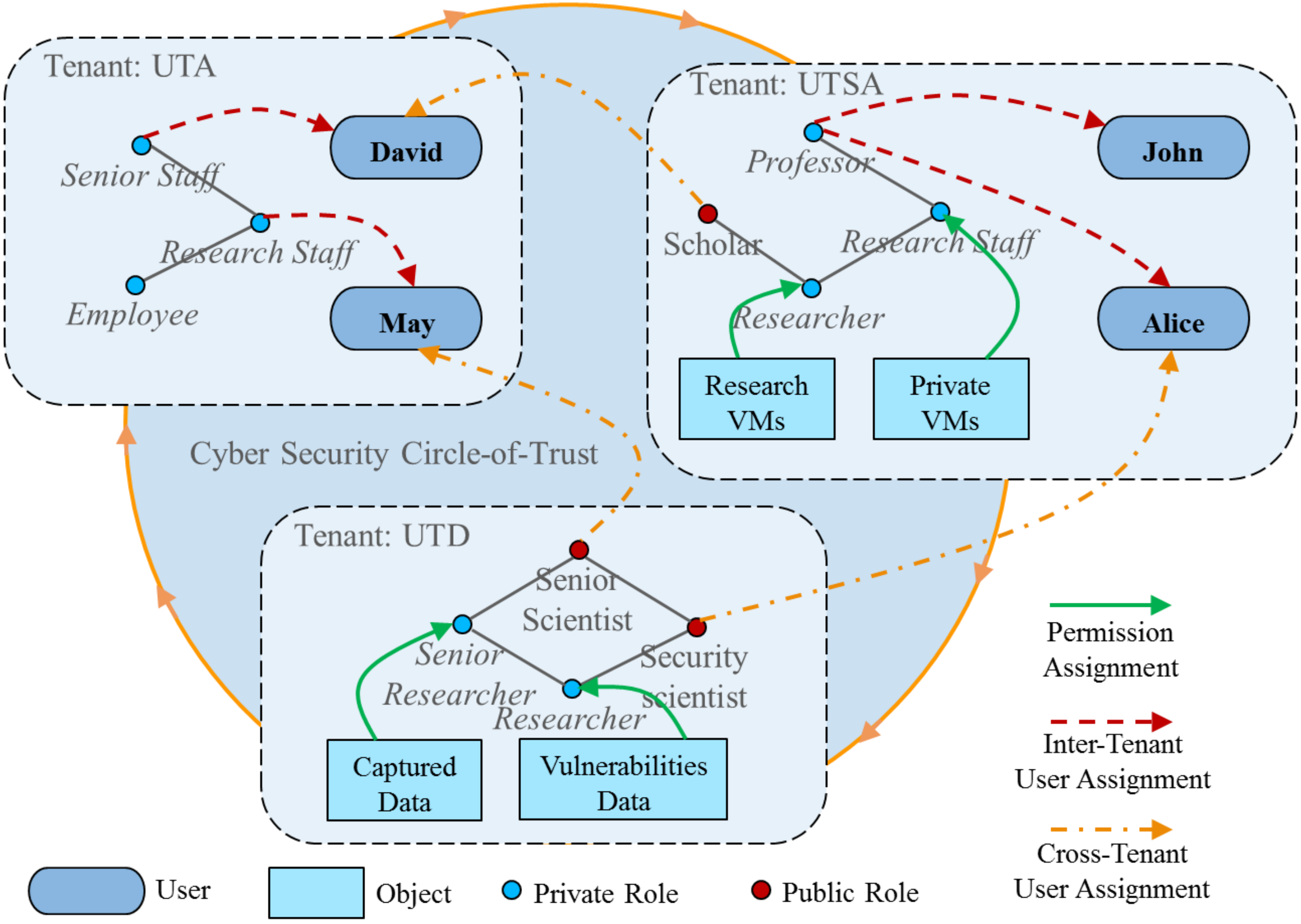
$Public\ Role_{T_B}1$

$Private\ Role_{T_B}2$ $Public\ Role_{T_A}3$

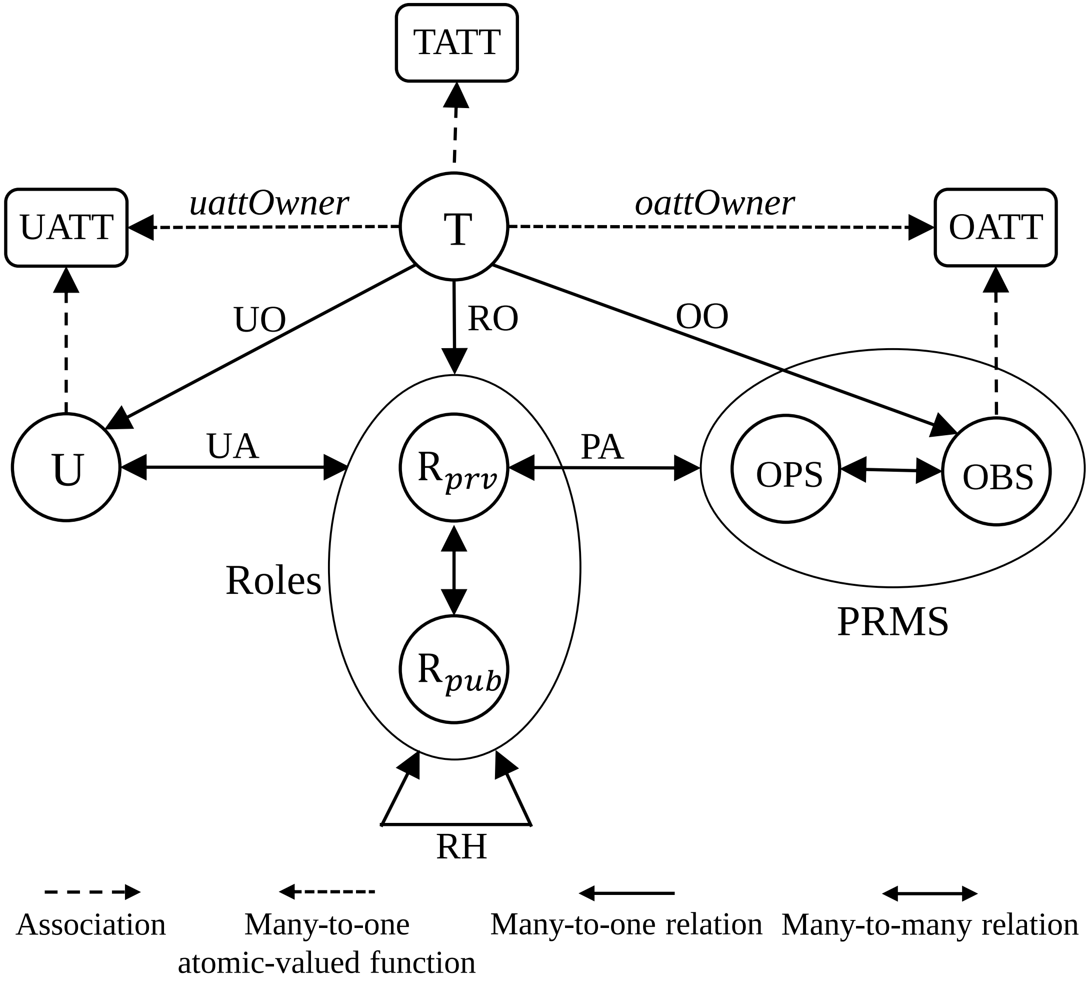
$Private\ Role_{T_B}4$ $Private\ Role_{T_A}5$ $Public\ Role_{T_A}6$

$Private\ Role_{T_A}7$

$MT-RBAC_c$ Use Case



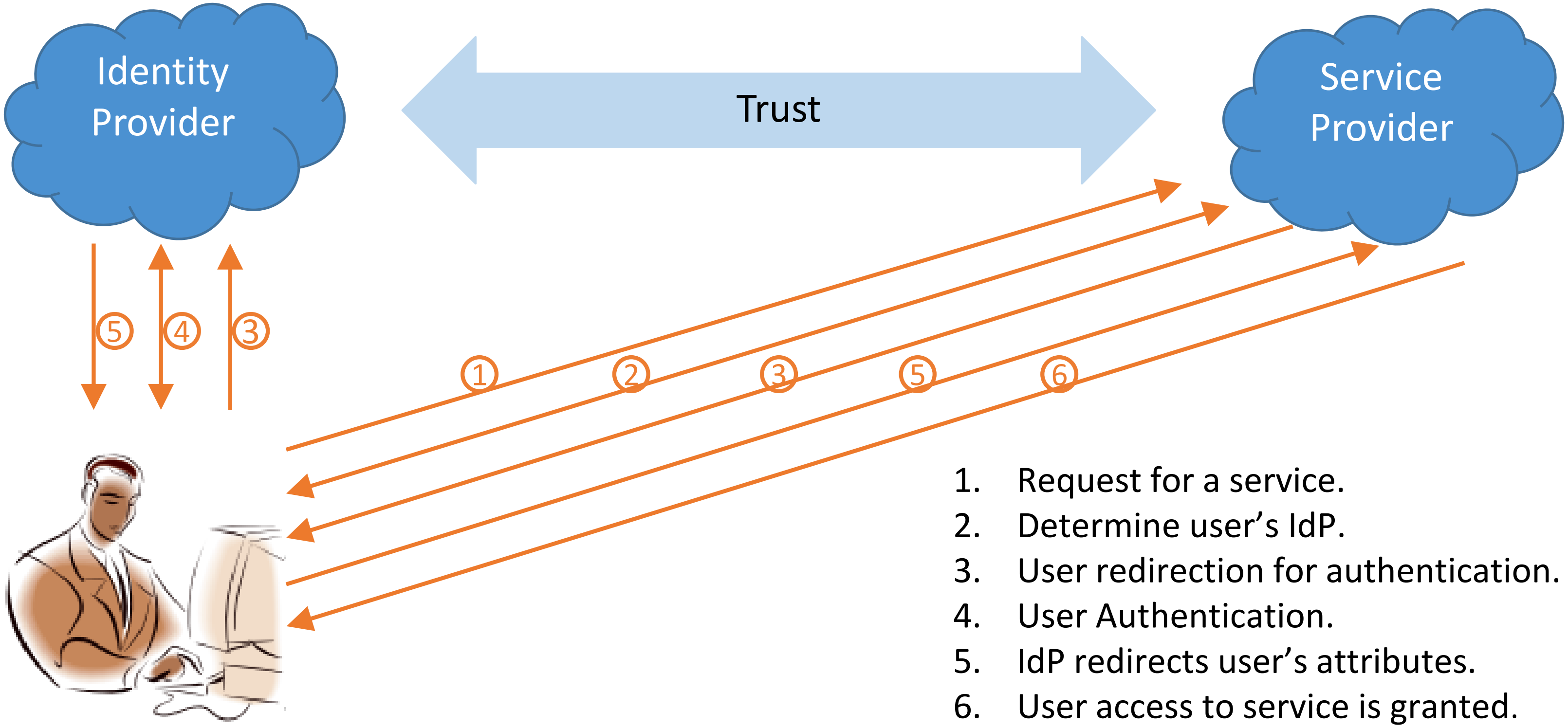
$MT - RABAC_c$



World-Leading Research with Real-World Impact!

Openstack Federation

- Adding Identity federation to OpenStack cloud, multiple identity providers can federate their users to an OpenStack cloud.

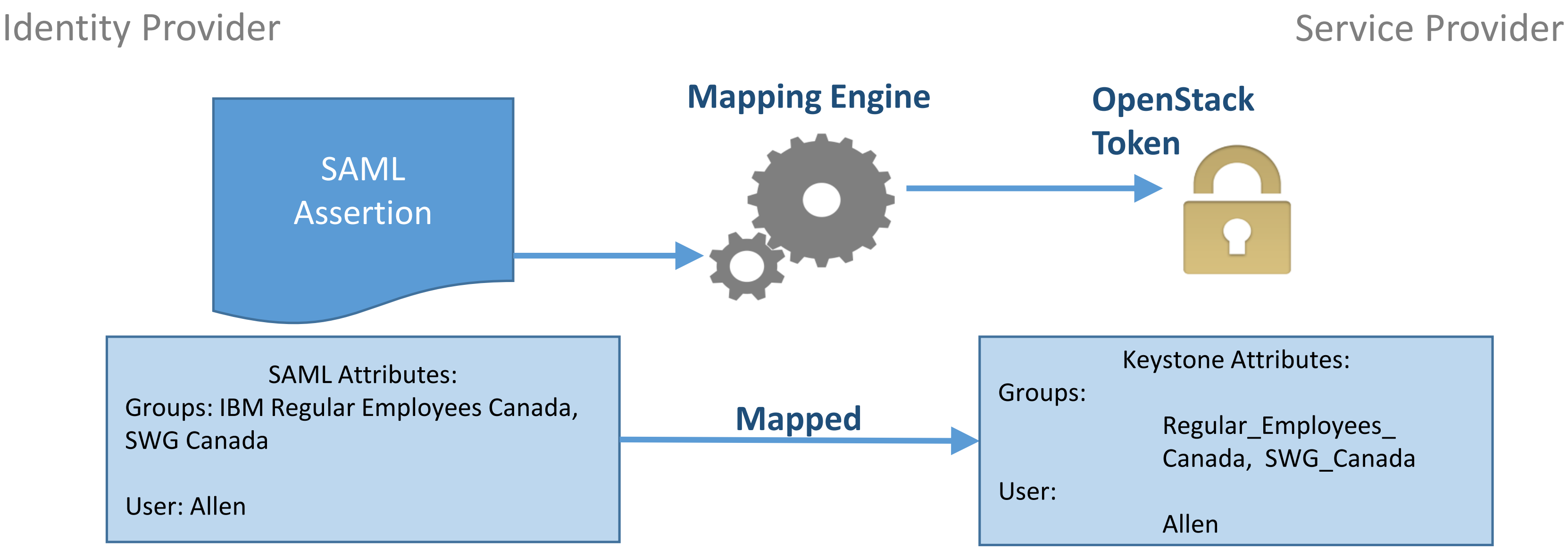


1. Request for a service.
2. Determine user's IdP.
3. User redirection for authentication.
4. User Authentication.
5. IdP redirects user's attributes.
6. User access to service is granted.

– CHADWK. (2014). Adding Federated Identity Management to OpenStack. Journal of Grid Computing, 2014.

Keystone Mapping Engine

- ➢ Takes SAML assertion as input, and as output OpenStack Token.
- ➢ OpenStack cloud admin creates a set of *mapping rules* which determines how to map SAML attributes to groups and users.



Identity Provider

Service Provider

SAML Assertion

Mapping Engine

OpenStack Token

SAML Attributes:
Groups: IBM Regular Employees Canada, SWG Canada

User: Allen

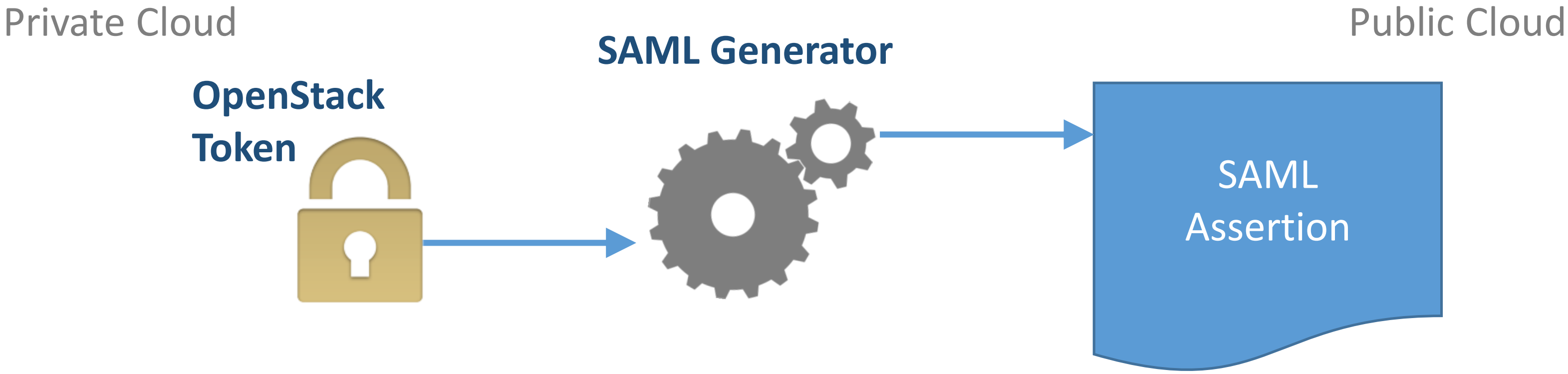
Mapped

Keystone Attributes:
Groups:
Regular_Employees_ Canada, SWG_Canada
User:
Allen

– OpenStack Paris Summit, Keystone to Keystone Federation, https://www.openstack.org/summit/openstack-paris-summit-2014/session-videos/presentation/keystone-to-keystone-federation, (2014)

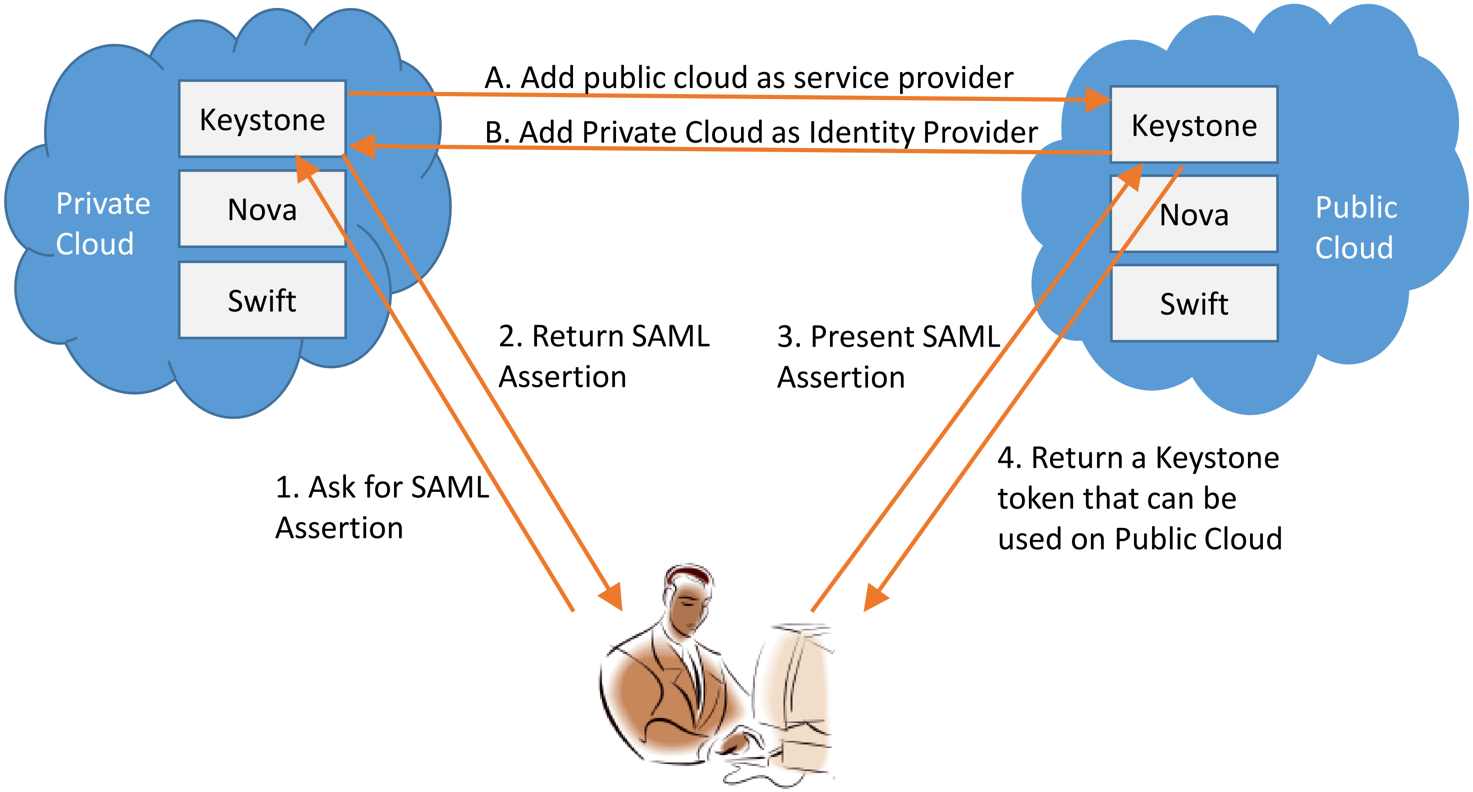
Keystone SAML Generator

- Takes as input: an OpenStack Token, and the service provider the user wants to use.
- Outputs a SAML Assertion that can be forwarded to the Service Provider.
- Assuming service provider has the Identity Provider created, the Private Cloud user should get a token that is valid at the Service Provider.



– OpenStack Paris Summit, Keystone to Keystone Federation, https://www.openstack.org/summit/openstack-paris-summit-2014/session-videos/presentation/keystone-to-keystone-federation, (2014)

Keystone to Keystone Federation


Private Cloud
Keystone
Nova
Swift
A. Add public cloud as service provider
B. Add Private Cloud as Identity Provider
Keystone
Nova
Swift
Public Cloud
2. Return SAML Assertion
3. Present SAML Assertion
1. Ask for SAML Assertion
4. Return a Keystone token that can be used on Public Cloud

– OpenStack Paris Summit, Keystone to Keystone Federation, https://www.openstack.org/summit/openstack-paris-summit-2014/session-videos/presentation/keystone-to-keystone-federation, (2014)

Questions ?

- Coarse-grained and fine-grained trust models in cloud.
  - Multi-Tenant Cloud.
  - Multi-Tenant Multi-Cloud.
- Peer-to-Peer Policy
  - Multi-cloud role-based model.
  - Multi-tenant attribute-based model.
- Circle-of-Trust Policy
  - Multi-tenant role-based access control model.
  - Multi-tenant role-centric attribute-based access control model.
- Implementation
  - Single-cloud tenant trust.
  - Federated-cloud tenant trust.