# Secure Information and Resource Sharing in Cloud

Yun Zhang, Ram Krishnan and Ravi Sandhu
Institute for Cyber Security and Department of Computer Science
The University of Texas at San Antonio, One UTSA Circle, San Antonio, TX 78249

## Abstract

The significant threats from information security breaches in cyber world is one of the most serious security problems. Organizations are facing growing number of sophisticated cyber-attacks every year. Efficient and securely share attack and security information during cyber incident response play more and more significant role in fixing the problems as well as helping organizations recover fast. While traditional systems are slow and inefficient in sharing information and resources securely, cloud platform provides us a great convenience to facilitate the sharing. In this paper, we propose access control models for secure information and resource sharing(IARS) in cloud of Infrastructure as a Service(IaaS).

## Introduction

The lacking of important attack and threat information sharing among organizations may lead to a big security breach. As organizations moving to cloud, we try to explore information sharing in cloud platforms.

Our motivation to build up a IARS model in IaaS came from the case of response to cyber incident. Consider a community cyber incident response scenario where organizations that provide critical infrastructure to a community (such as a city, county or a state) share information related to a cyber incident in a controlled manner [1]. Sharing information amongst such organizations can greatly improve the resilience of increasingly cyber-dependent communities in case of co-ordinated cyber attacks [2]. A effective cyber incident response mechanism need to be build up to provide organizations technique support and services to handle the problems once the cyber incident happens.

## Background

OpenStack is a open source cloud platform of IaaS. OpenStack software controls large pools of compute, storage, and networking resources throughout a datacenter [3]. It provides several services, including compute (Nova), identity (Keystone), block storage (Cinder), object storage (Swift), image (Glance), networking (Neutron) and Dashboard (Horizon). In paper [4], the authors present a core OpenStack Access Control (OSAC) model, as shown in figure 1. The OSAC model consists of eight entities: users, groups, projects, domains, roles, services, operations, and tokens.

## OSAC-SID Model

We extend the OSAC model to include SID and SIP components, as shown in figure 2. In the OSAC-SID model, we assume that a user can belong to only one organization, which is consistent with the user and home-domain concept in OpenStack. For every possible combination of organizations in the cloud, we create a SID to include all SIPs that will be set up among these organizations. For each IARS event, we create a SIP.

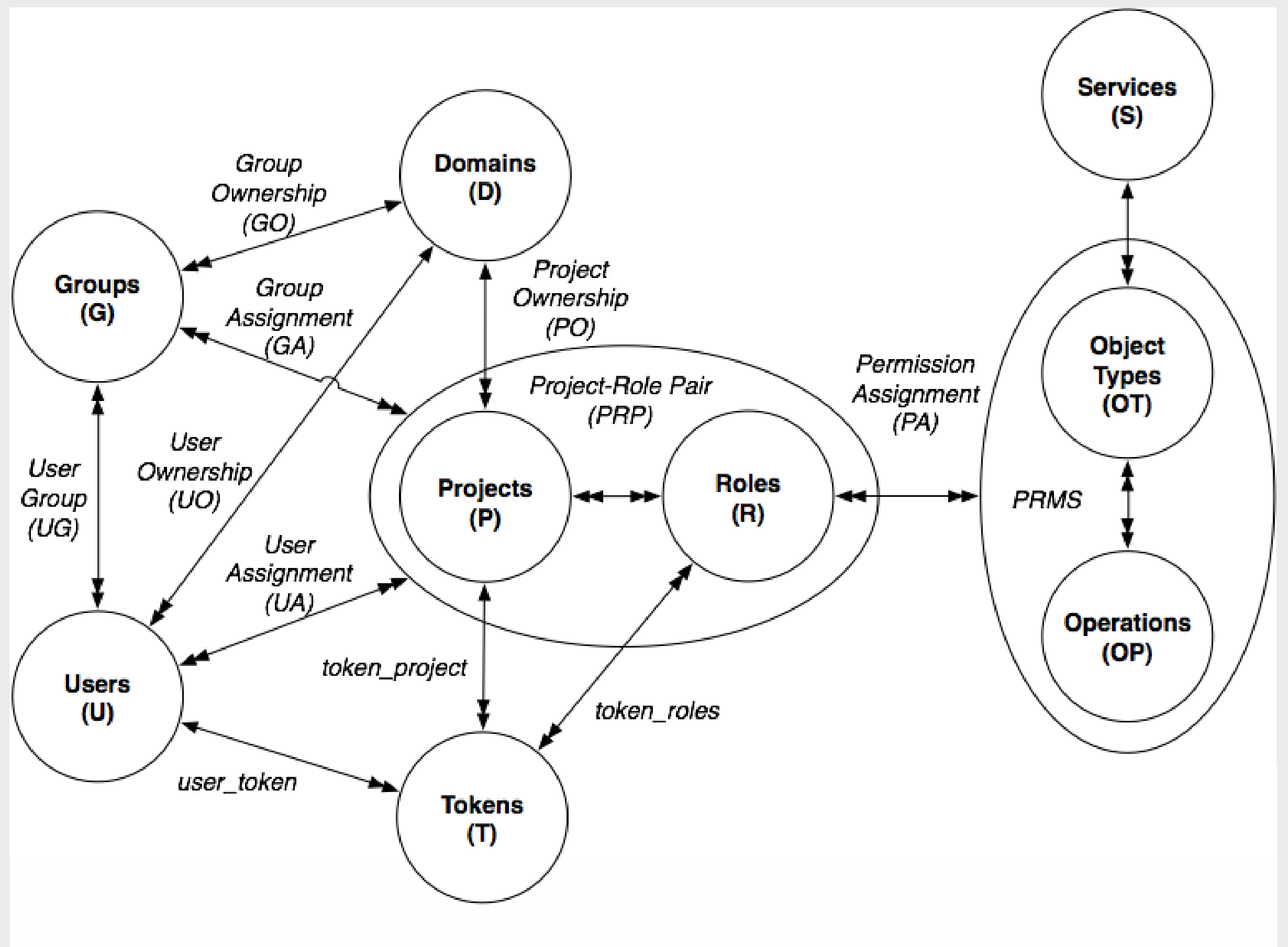

Figure 1. OpenStack Access Control (OSAC) model [4]

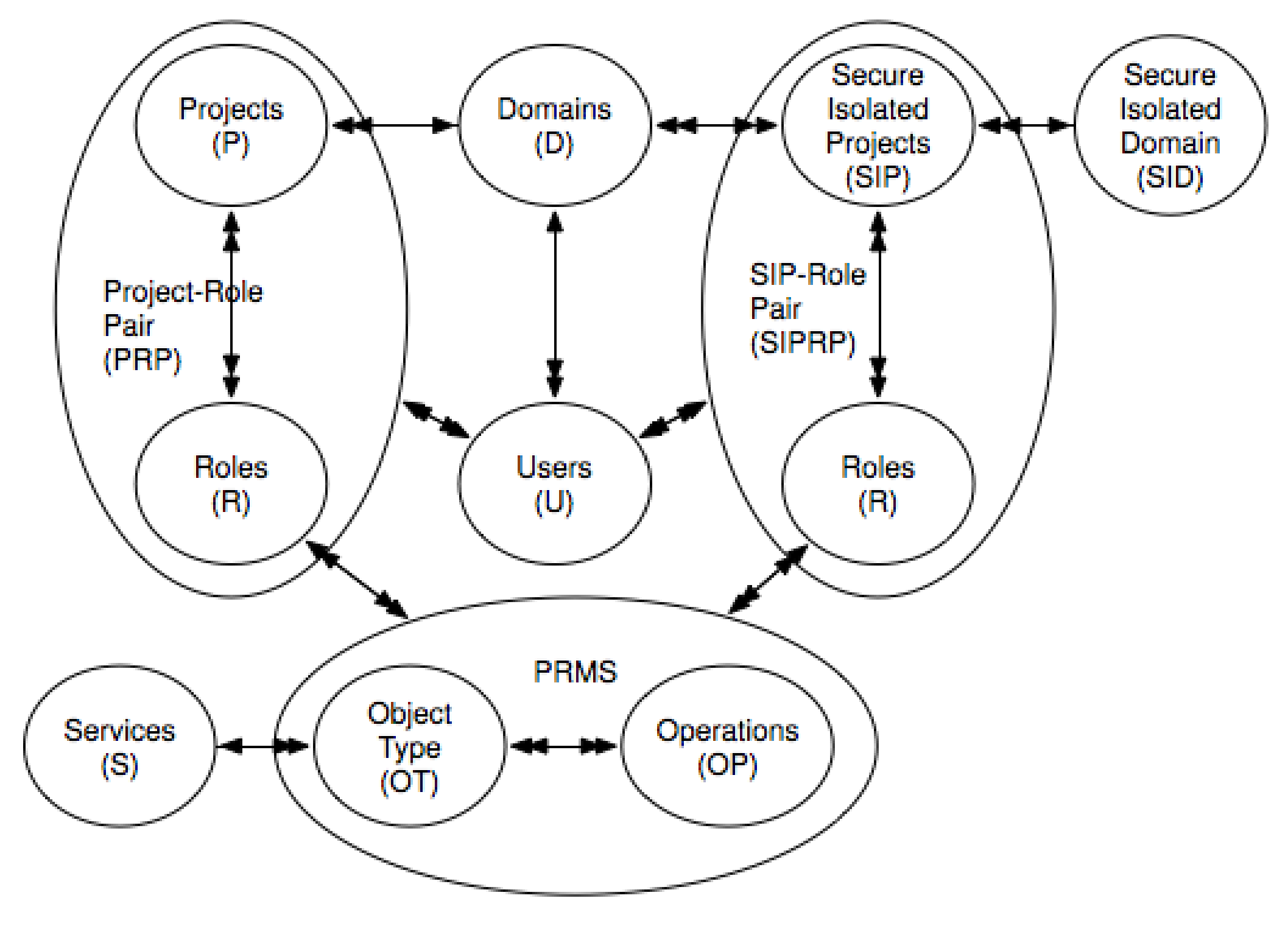

Figure 2. OpenStack Access Control (OSAC) model with SID extension(ignore group and token entities)

SID is an administrative concept to manage SIPs. SID and SIP entities are isolated from the regular domain and projects components. Unlike the concept of domains, there are no users that belong to a SID. A SID exists only for setting up SIPs. However, since a SID is formed and associated with a group of domains, there are users who will be associated with the SID---but only under the constrains that they are from the group of domains which are associated with the SID.

A SIP provides a secure isolated space for secure IARS in the cloud. In other words, SIP is another type of resources container in OpenStack, which is restricted only for IARS among domains and projects. It means that users who are assigned to a SIP have similar access capability to request all services cloud provides like users who are assigned to a project. We define OSAC-SID model by inheriting some of the attributes of OSAC model discussed earlier. For simplicity, we choose to ignore two entities in OSAC model: group and token, for reasons that group entity is just a set of users, and token is used in the same way as for a domain/project and for a SID/SIP.

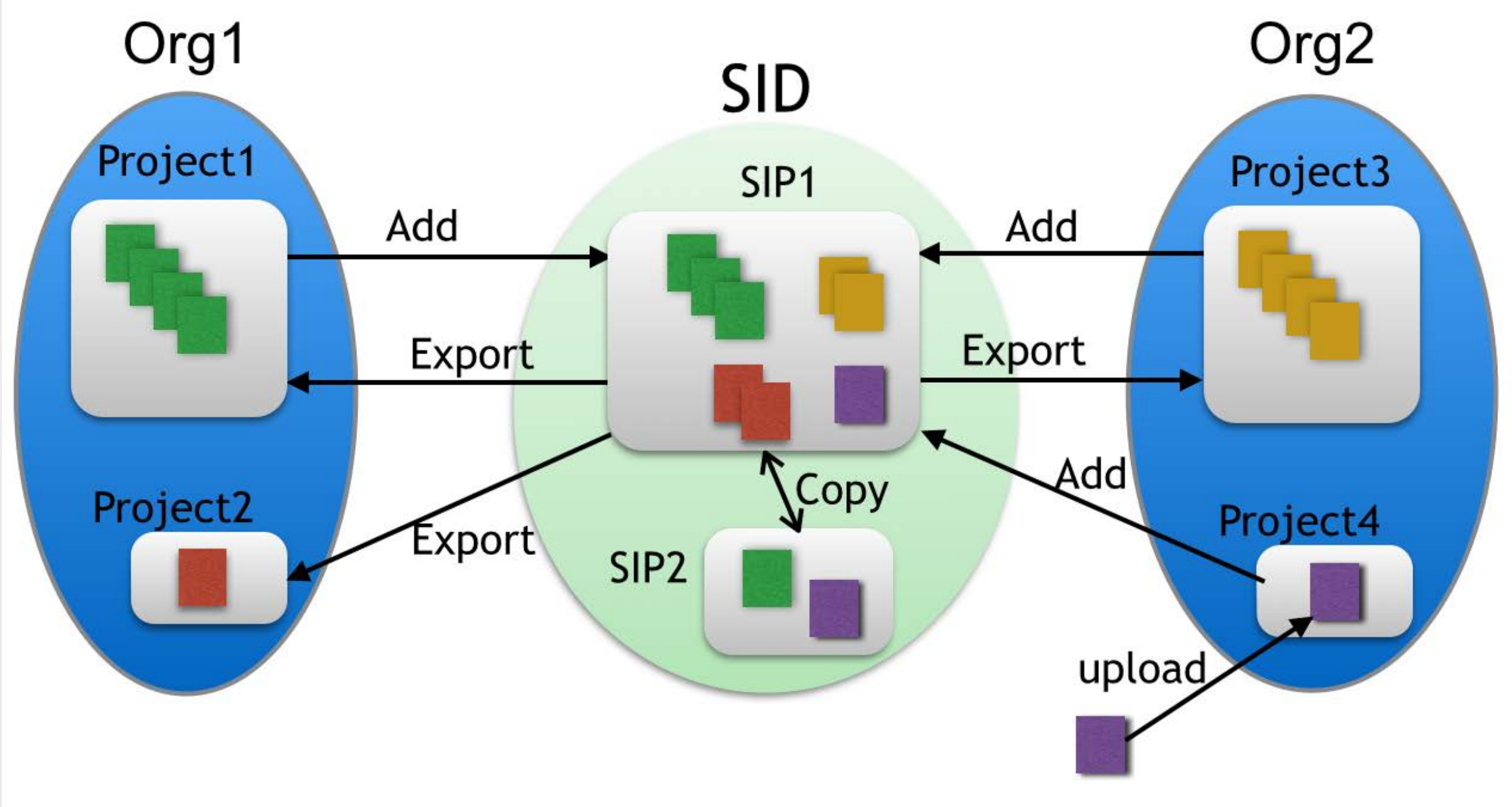

Figure 3. Establish a SID

## Implementation

In order to deploy the model in OpenStack platform, we need to modify Keystone entity to include SID and SIP functionality in OpenStack, which facilitate features of IARS. SID functionality include SID creation, updating and deletion, and so on. SIP functionality allows users bring in their data and utilize the cloud resources to process the data. It provides users full access to the resource inside a SIP, where a user can create, update, delete and copy an object.

We assume that each domain represents an organization in OpenStack while projects inside a domain could represent a department or temporary project in the organization. In the case of collaboration, multiple organizations would form a group to create a SID. SIPs will be created inside the SID to facilitate collaboration for different reasons. Objects are exchanged among organizations and SIPs under restrains of policy of SID. Figure 3 gives a simple view of how SID is established among organizations, we assume we have Org1 and Org2.

We implement the model in OpenStack icehouse release. To establish a sid, we need to modify two parts in OpenStack: Policy and Keystone. The sid/sip establishment steps: 1) A domain admin initiate a sid creation with parameter of uSet which includes itself; 2) Domain admins who belongs the uSet assign themselves the sid admin role to the sid; 3) Sid admins create sips and assign users from their home domains to any sips inside the sid. Figure 4 shows the whole sid/sip establishment process. After the sid/sip is established, users can start operation inside sid/sip as well as between sid/sip and their home projects.

Figure 5 gives an example of establishing a sid with sips between two organizations: CPS and SAWS. We assume all these three organizations sitting in the same cloud IaaS platform. Organization SAPD is not participating the collaboration of cyber incidents. Organizations CPS and SAWS forms the collaboration group for working on projects: PortScanning and DOS attack.

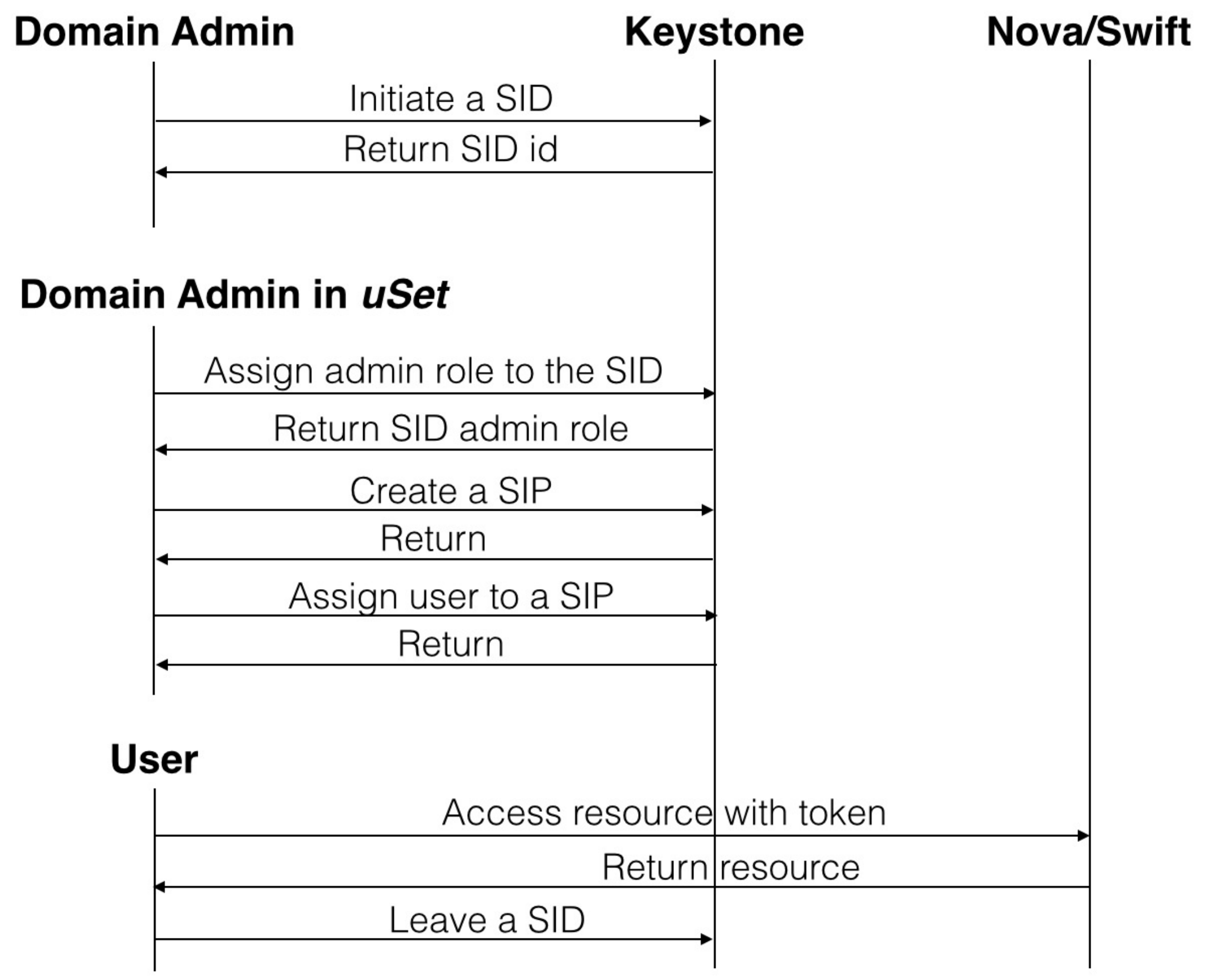

Figure 4. Sid/Sip establishment Process [5]

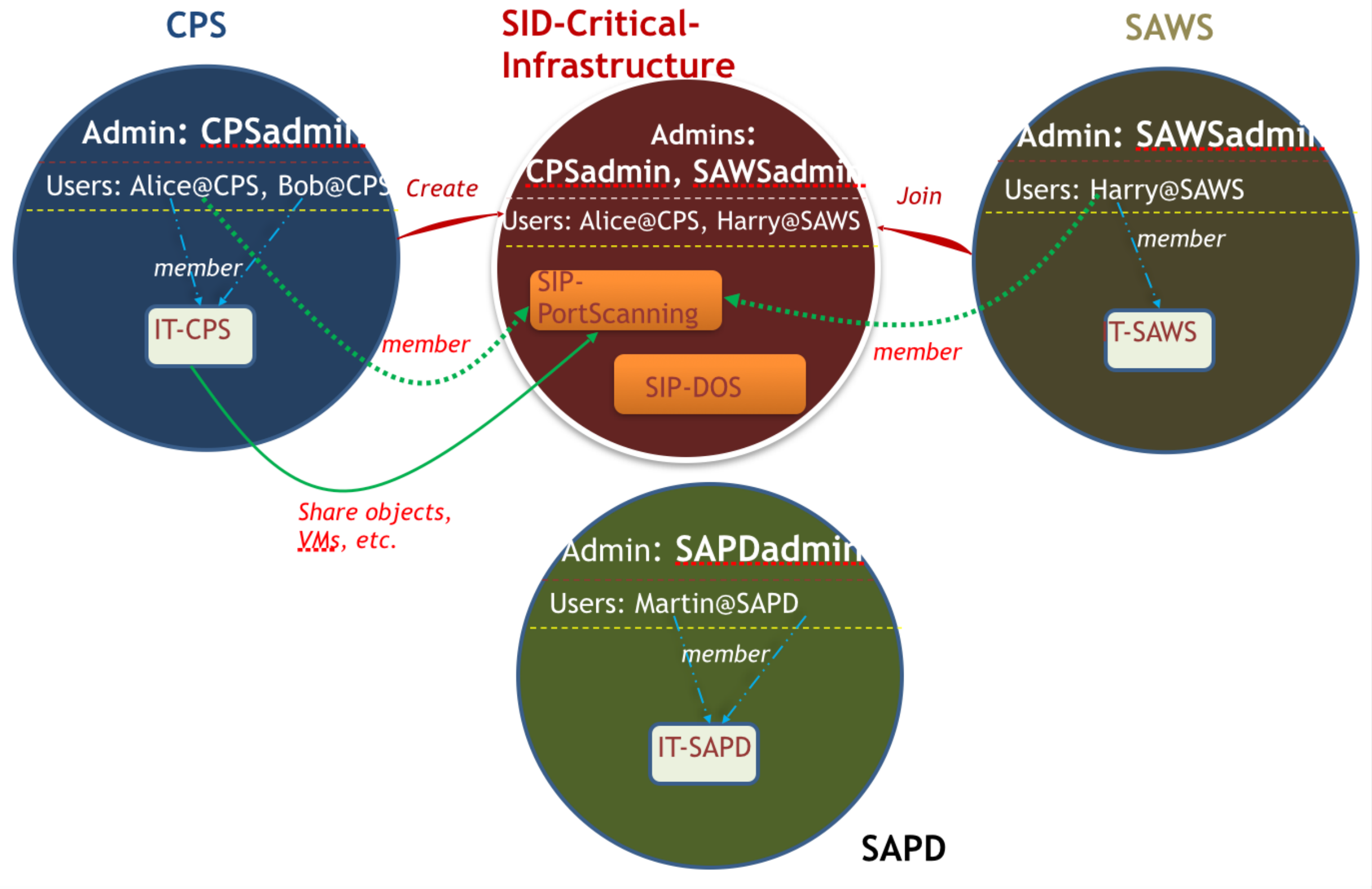

Figure 5. Sid/Sip establishment Example [5]

## Conclusions

We developed a model for IARS. For the future work, we plan to investigate fine-grained access control within a SIP.

## References

[1] K. Harrison and G. White. Information sharing requirements and framework needed for community cyber incident detection and response. In Homeland Security (HST), 2012 IEEE Conference on Technologies for, pages 463–469, Nov 2012.
[2] K. Harrison and G. B. White. Anonymous and distributed community cyberincident detection. IEEE Security and Privacy, 11(5):20–27, 2013.
[3] http://openstack.org.
[4] B. Tang and R. Sandhu. Exteding openstack access control with domain trust. In Proceedings 8th International Conference on Network and System Security (NSS 2014), October 15-17 2014.