

INFORMATION SHARING IN CLOUD

Amy(Yun) Zhang

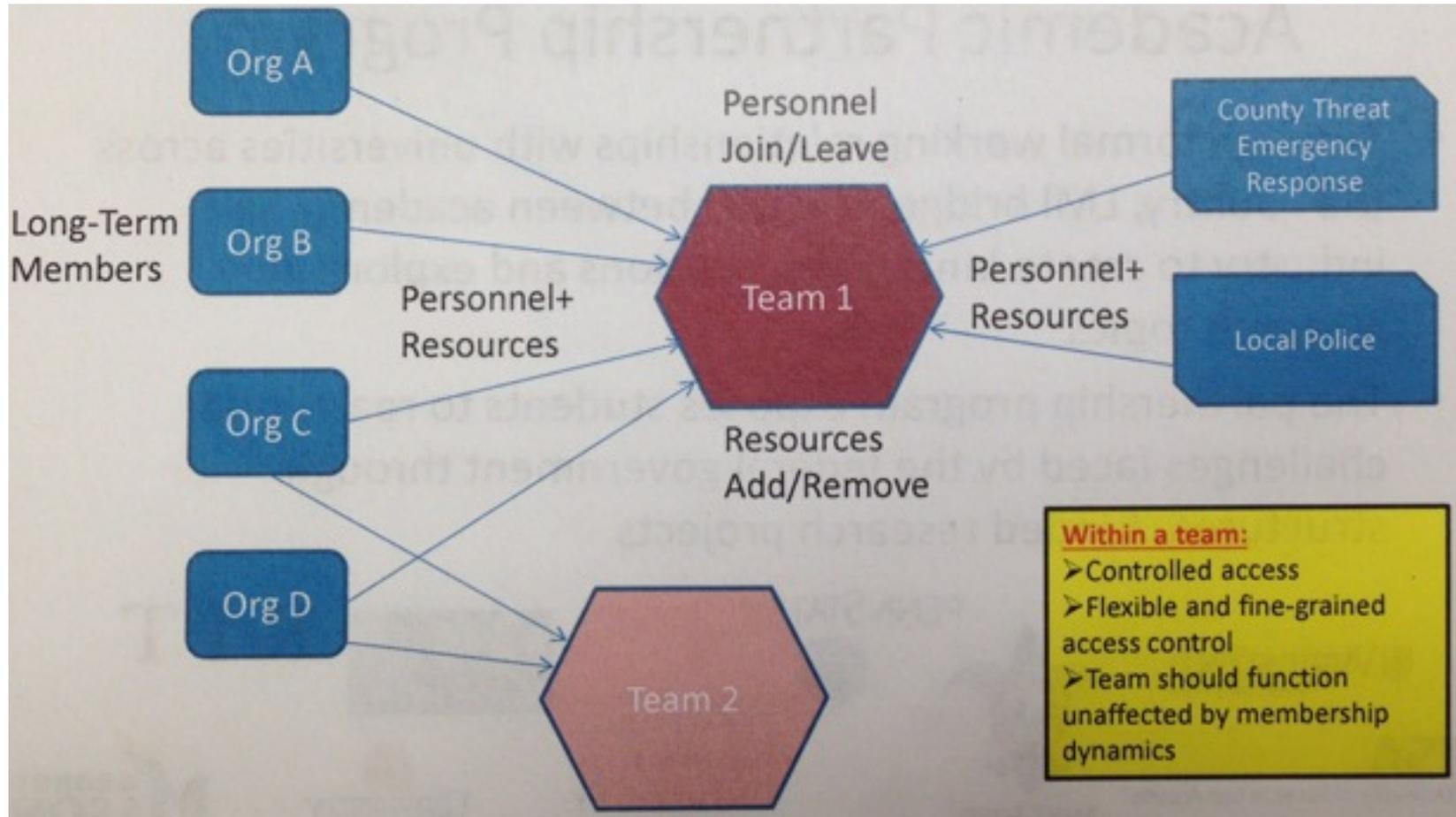
Presented by Amy

May 1, 2014

ICS-UTSA

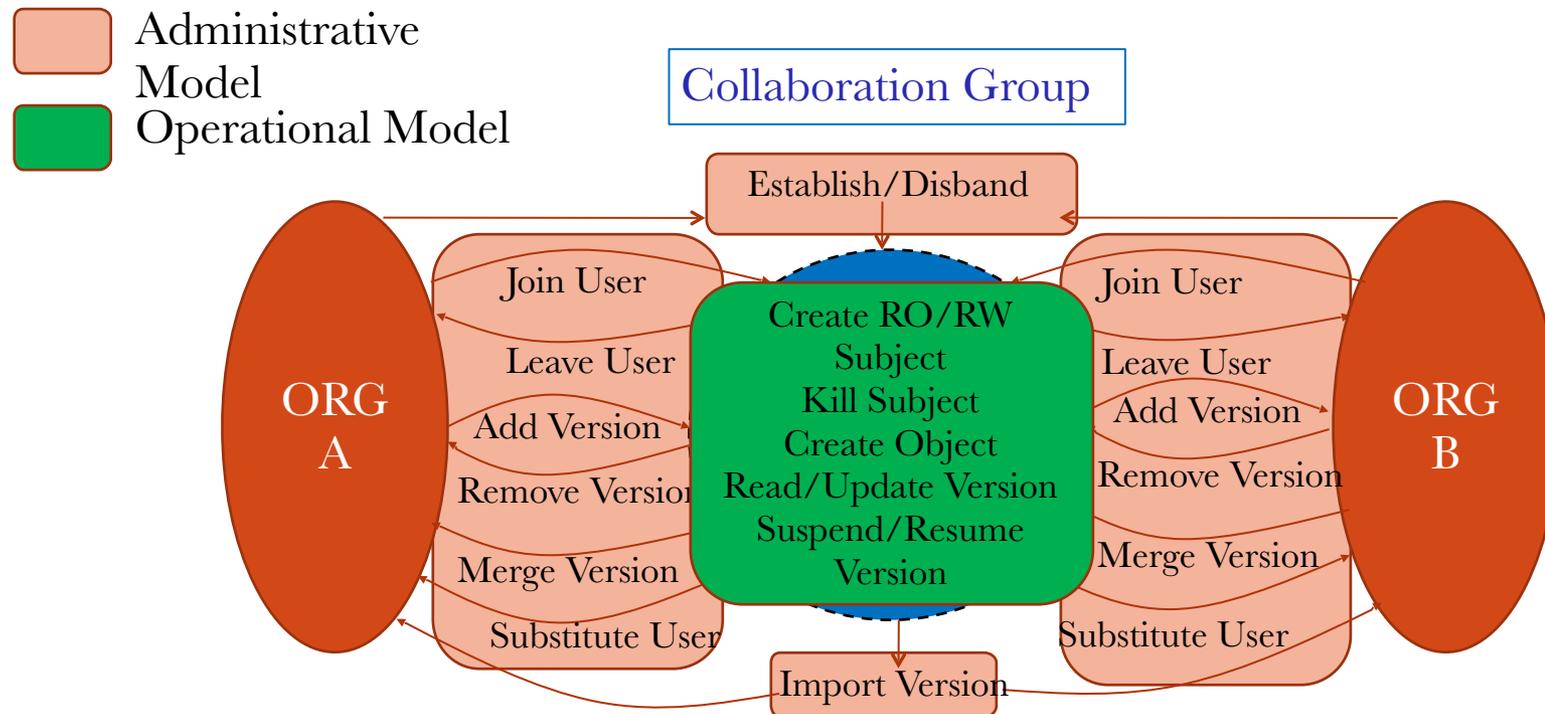
- Cyber security incident response
 - ❖ share information securely amongst a set of entities/organizations
 - » often ad hoc
 - » sensitive information involved
 - » need a isolated domain to do the collaboration

➤ Agile Incident Response



cited from presentation of Dr. RAM

- Systematically study authorization aspects in a simple inter-organizational collaboration scenario



- cited from presentation of paper <Towards a Framework for Group-Centric Secure Collaboration>

➤ secure information sharing for cyber incident response

❖ high assurance (closed network)

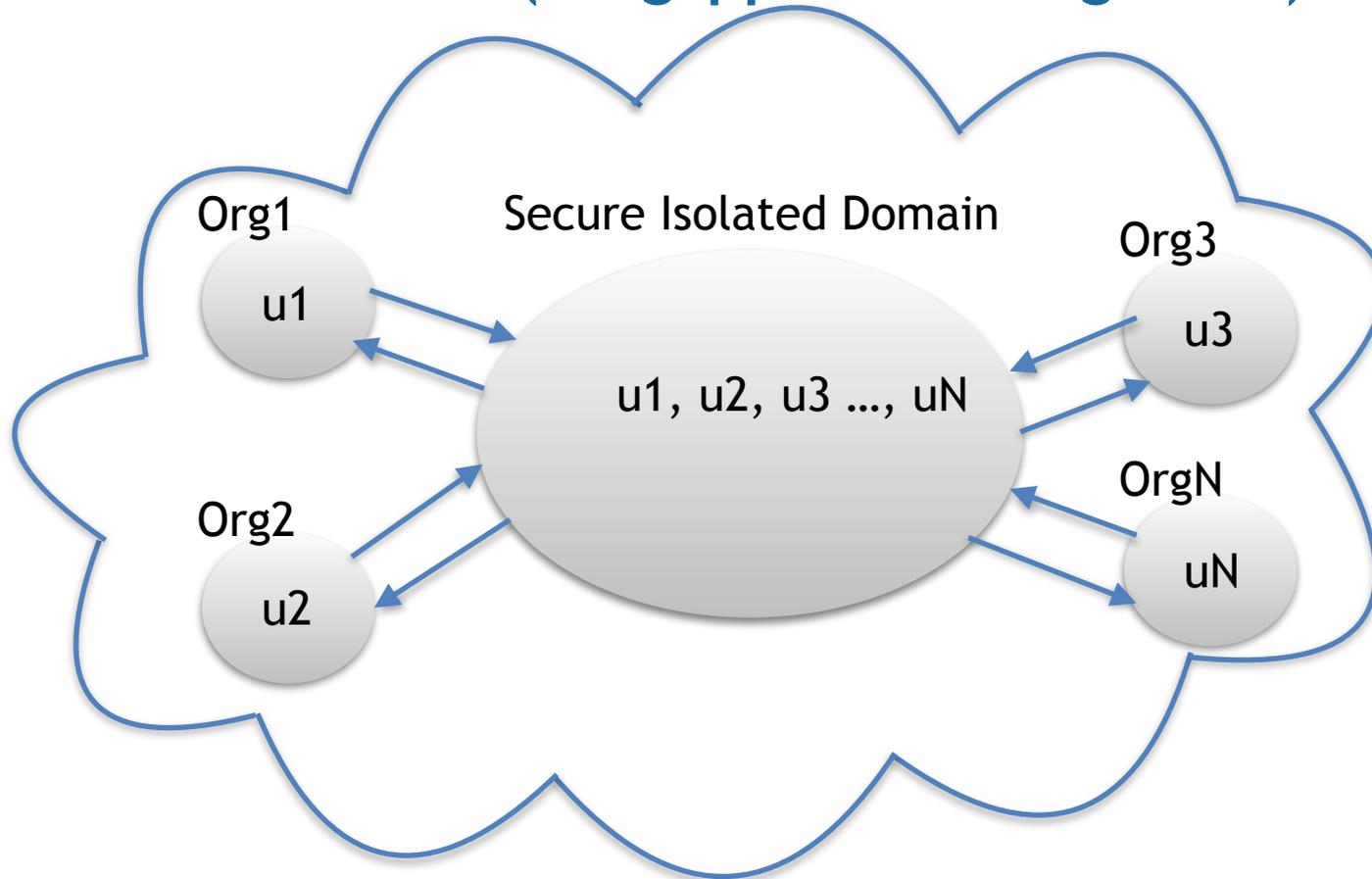
- » unusual activity in military(Air Force, Navy & Army) networks
- » a physically secure and air-gapped meeting room with members from corresponding military organizations
- » member bring sensitive data for analysis and collaboration
- » strict control on data import/export

❖ medium assurance (community)

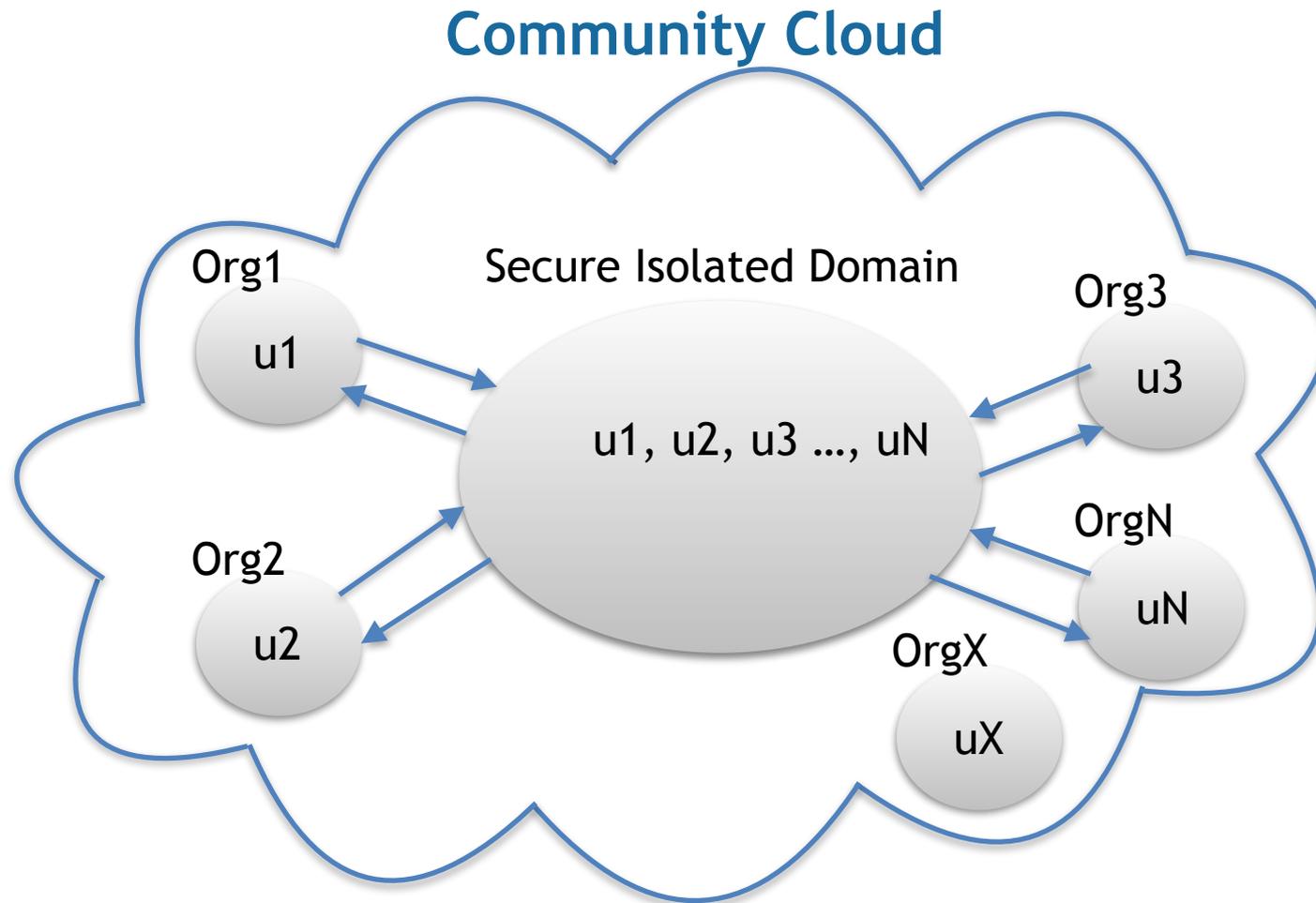
- » Cyber incidents across critical infrastructure providers in a community
 - emergency response, healthcare, banks, utility
 - » Need a community information sharing platform
 - controlled access
-

➤ High-assurance scenario

Cloud in a box(air-gapped meeting room)

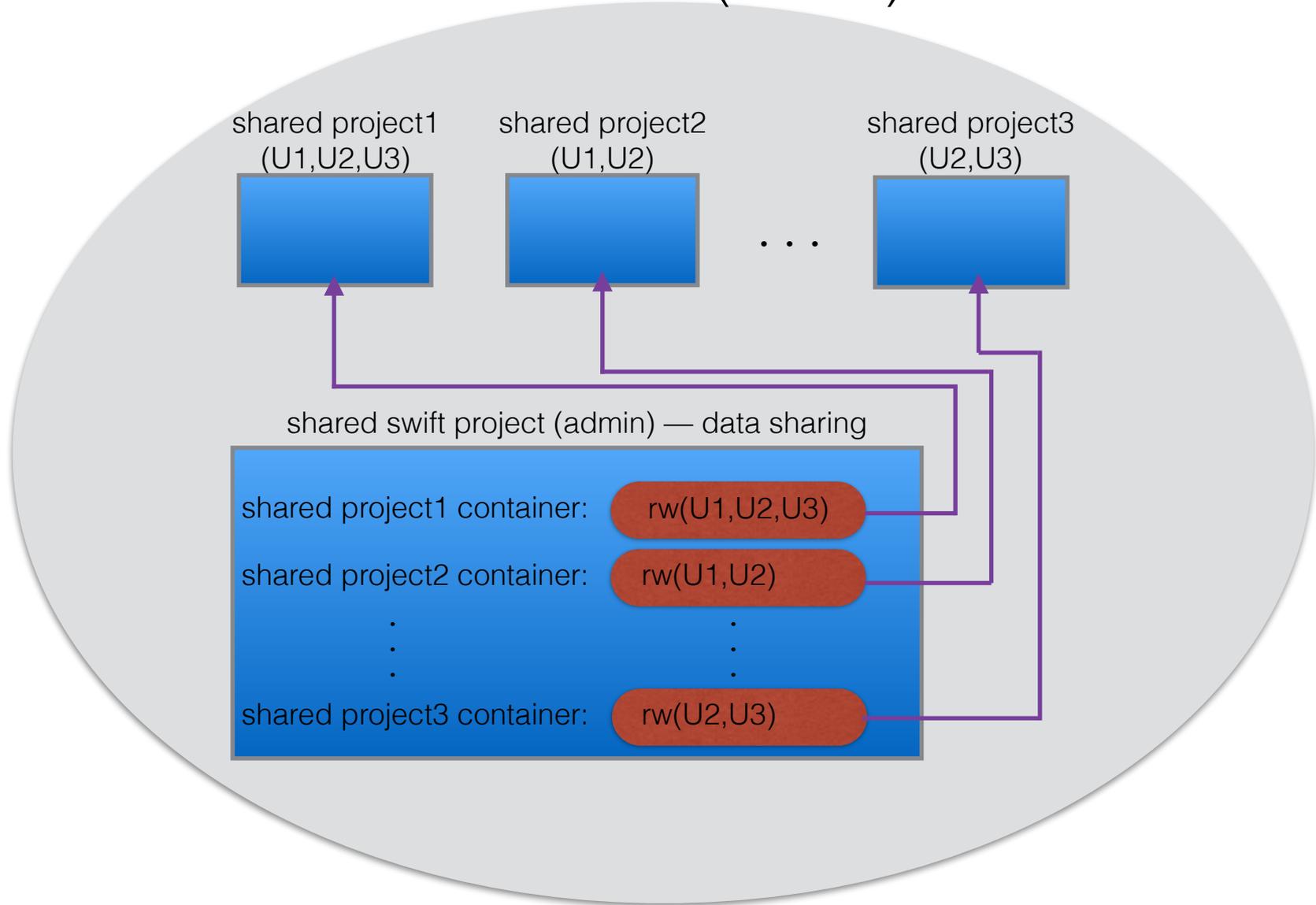


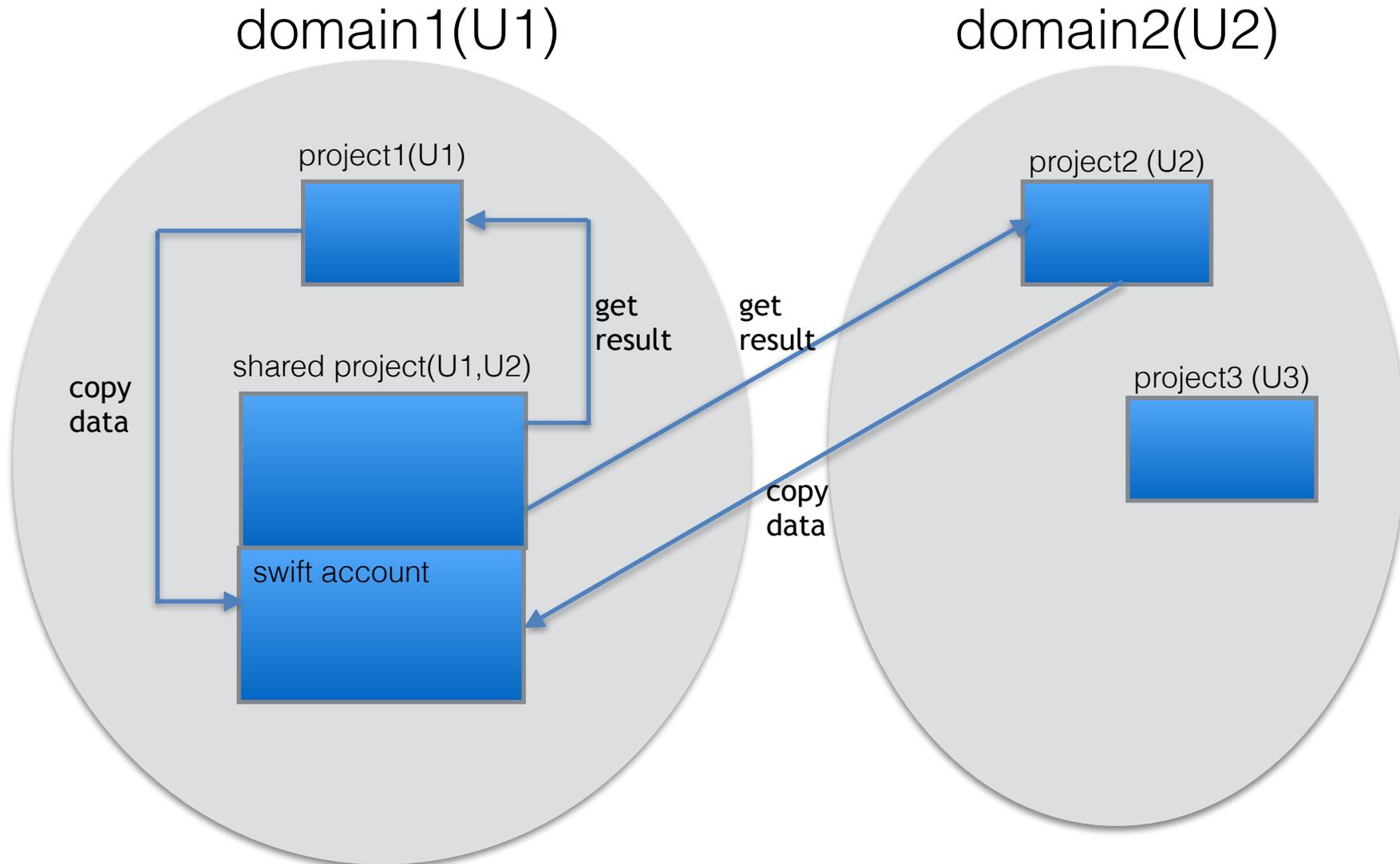
➤ Medium-assurance scenario



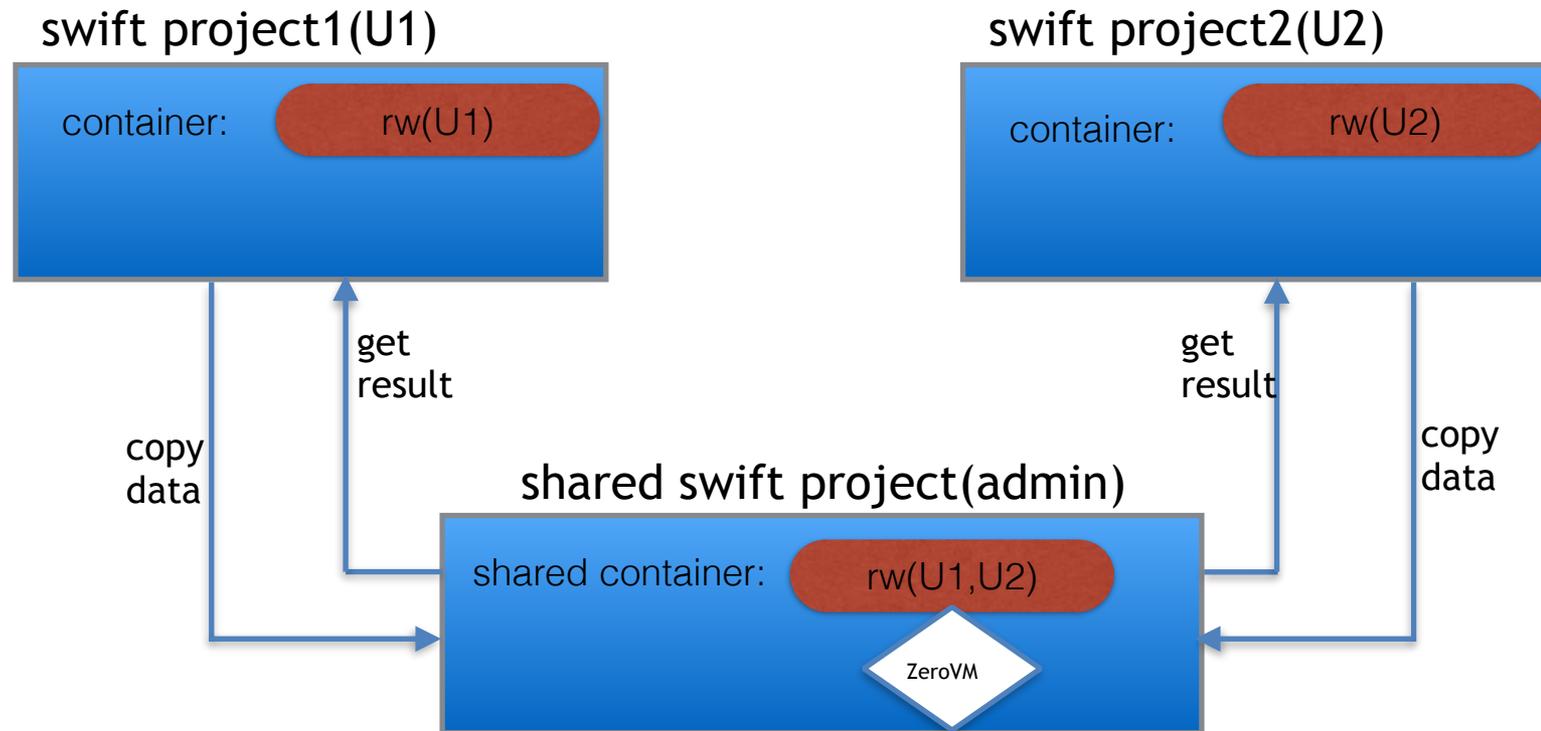
Proposed Models of High-Assurance Scenario (Cloud-in-a-box)

domain (admin)



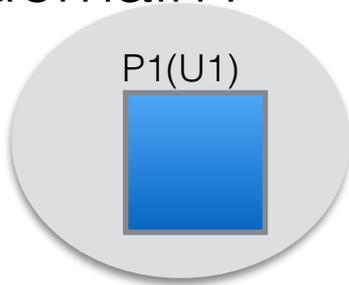


- shared container in swift
- utilize Zero-VM

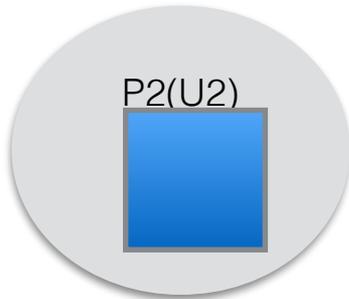


Proposed Models of Medium-Assurance Scenario

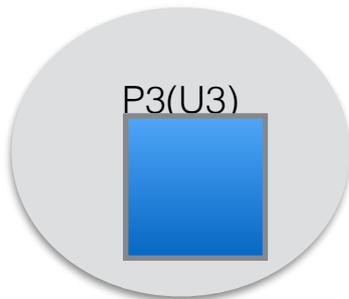
domain1



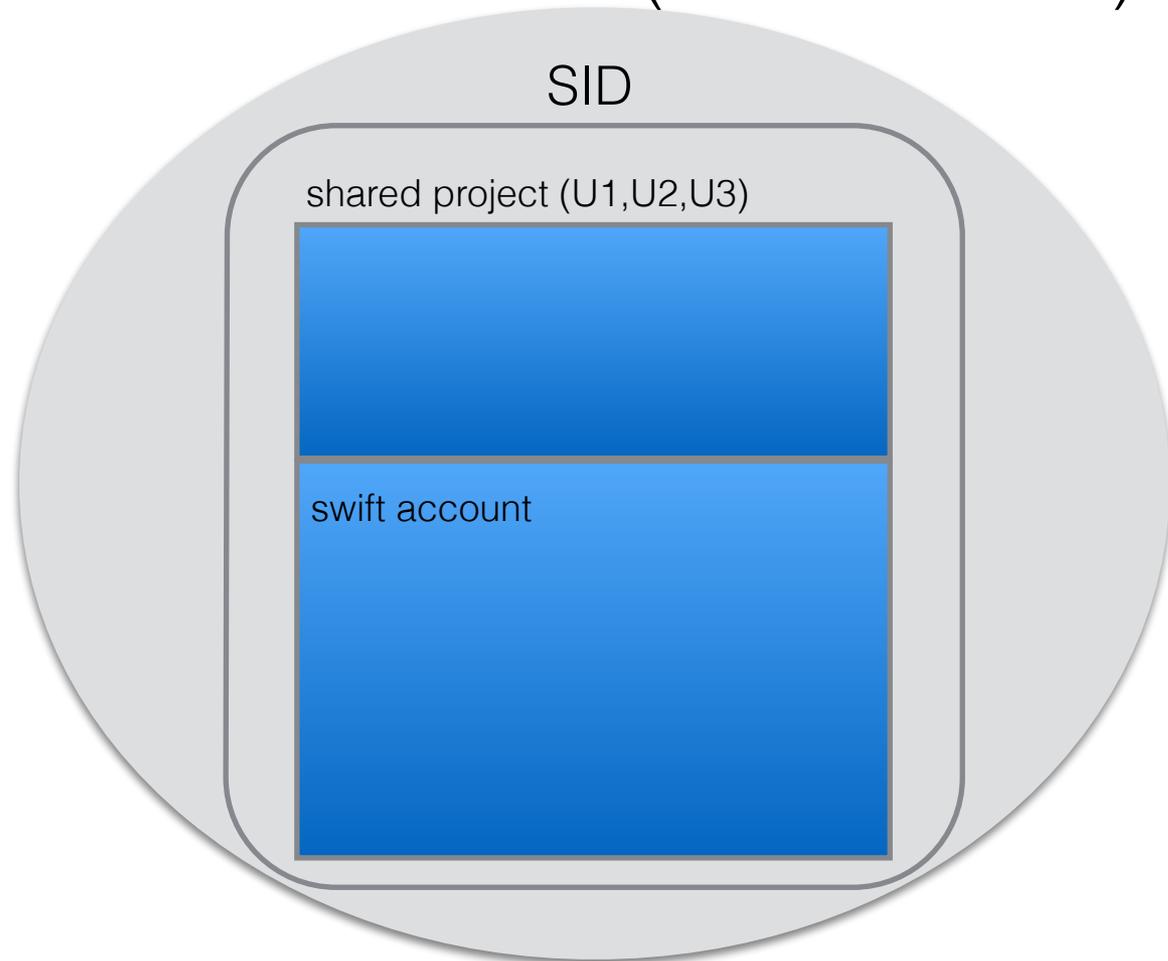
domain2



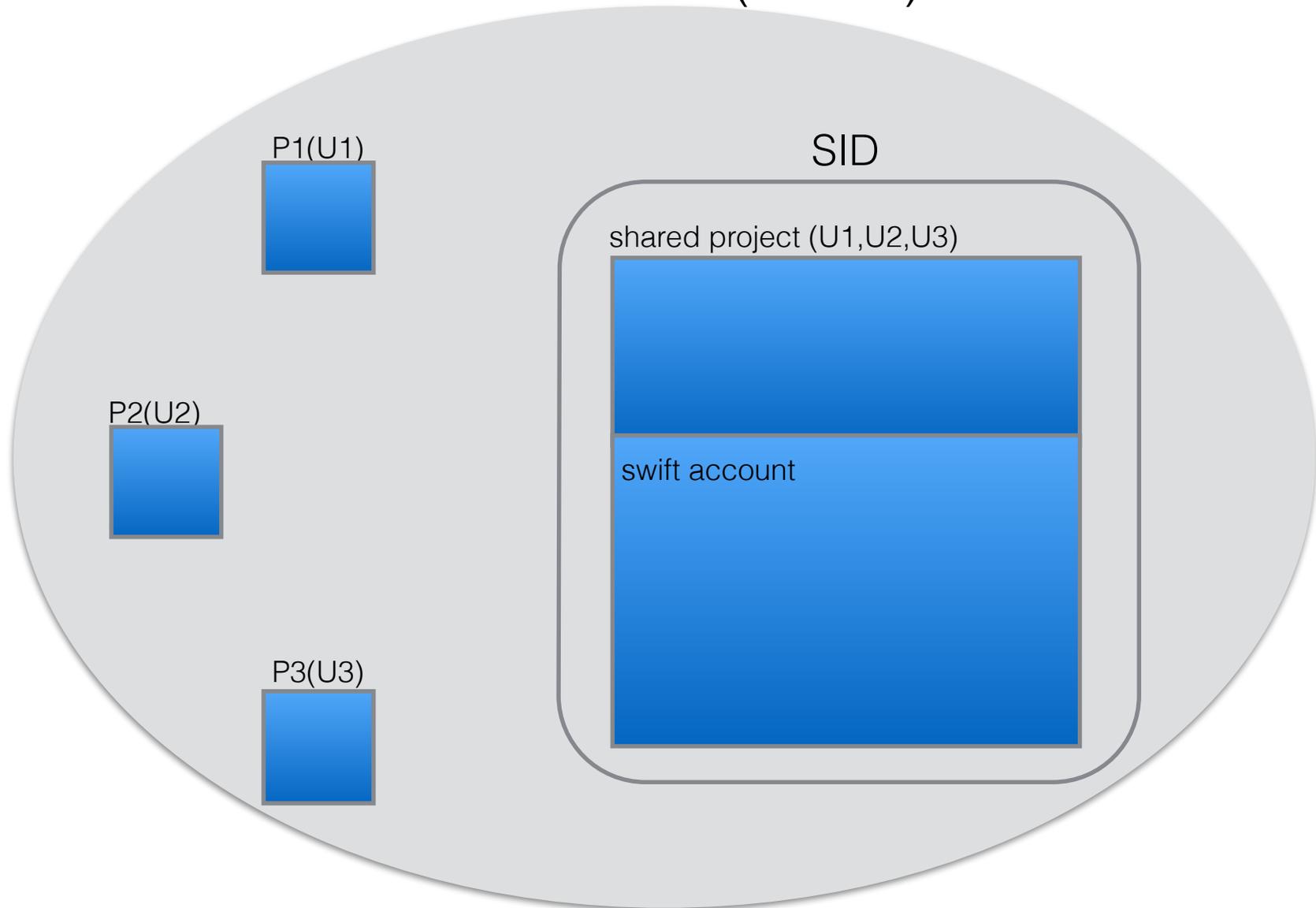
domain3

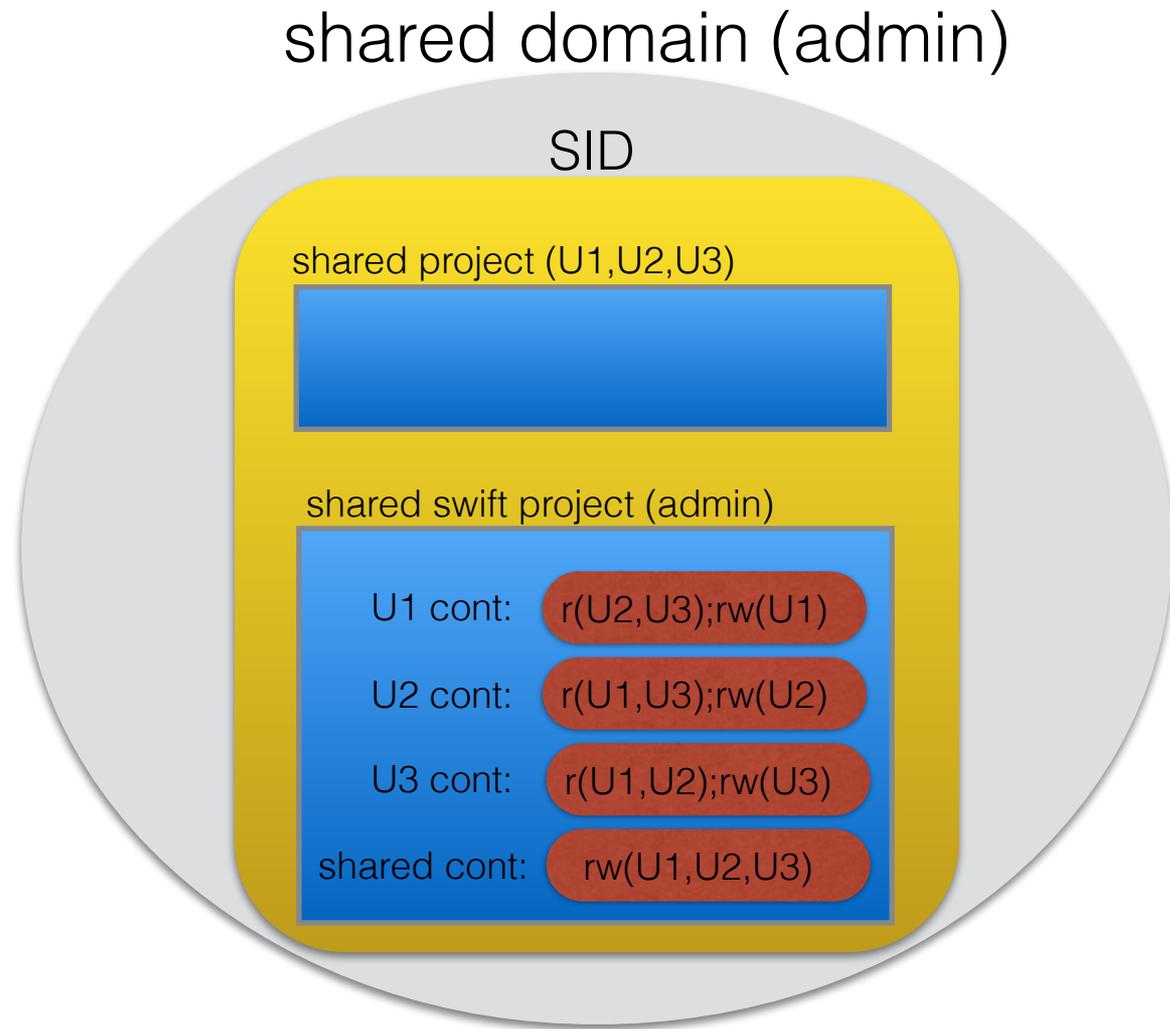
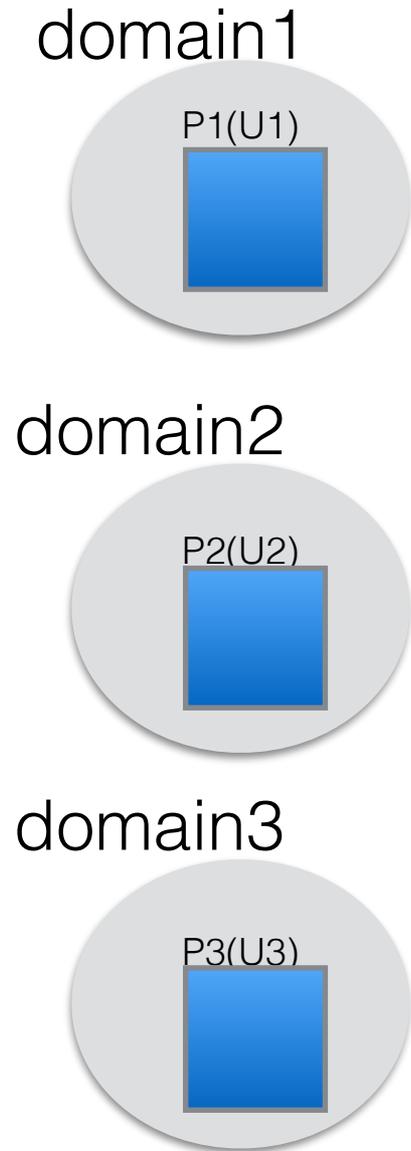


shared domain (domain admin)

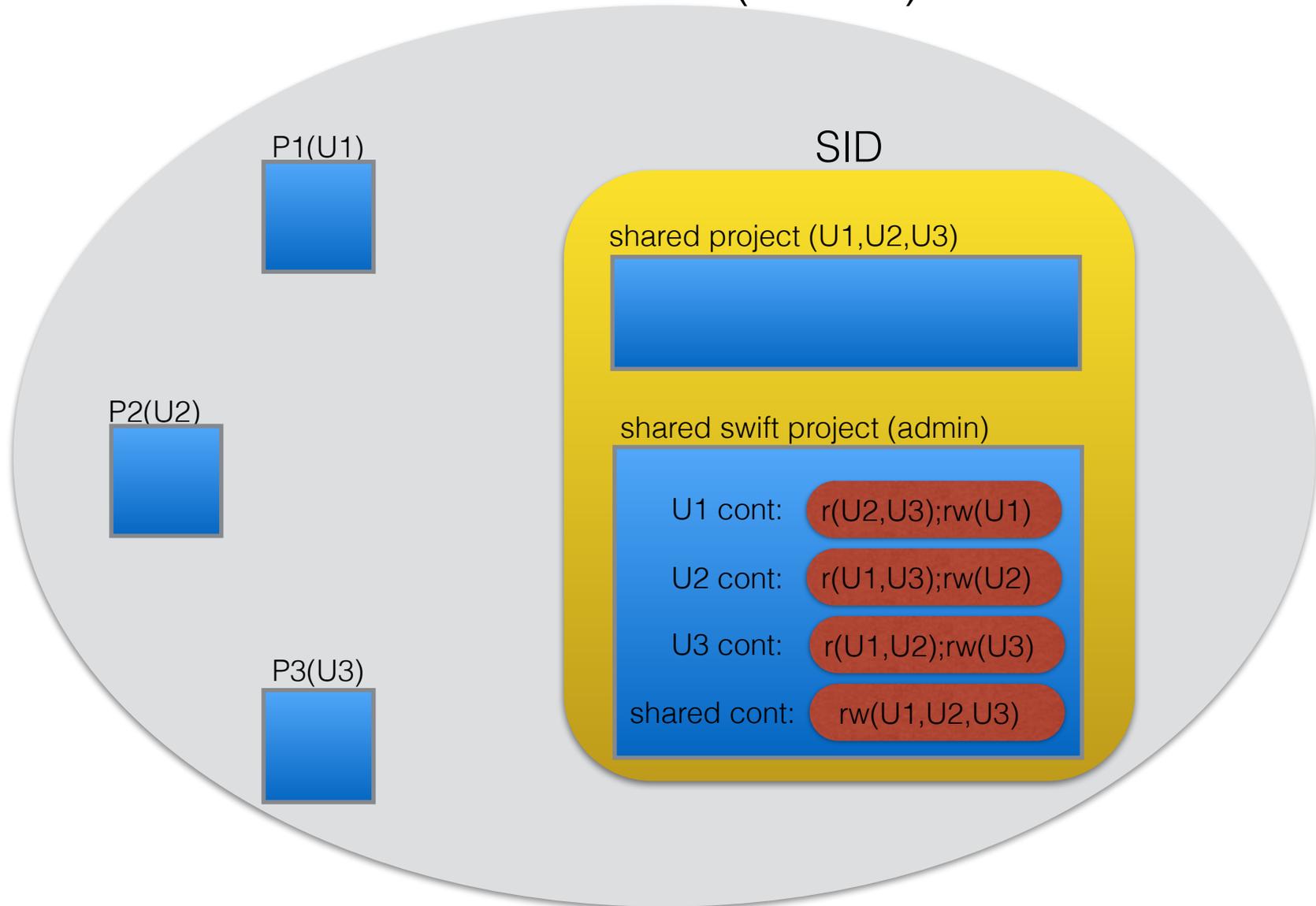


domain (admin)





domain (admin)



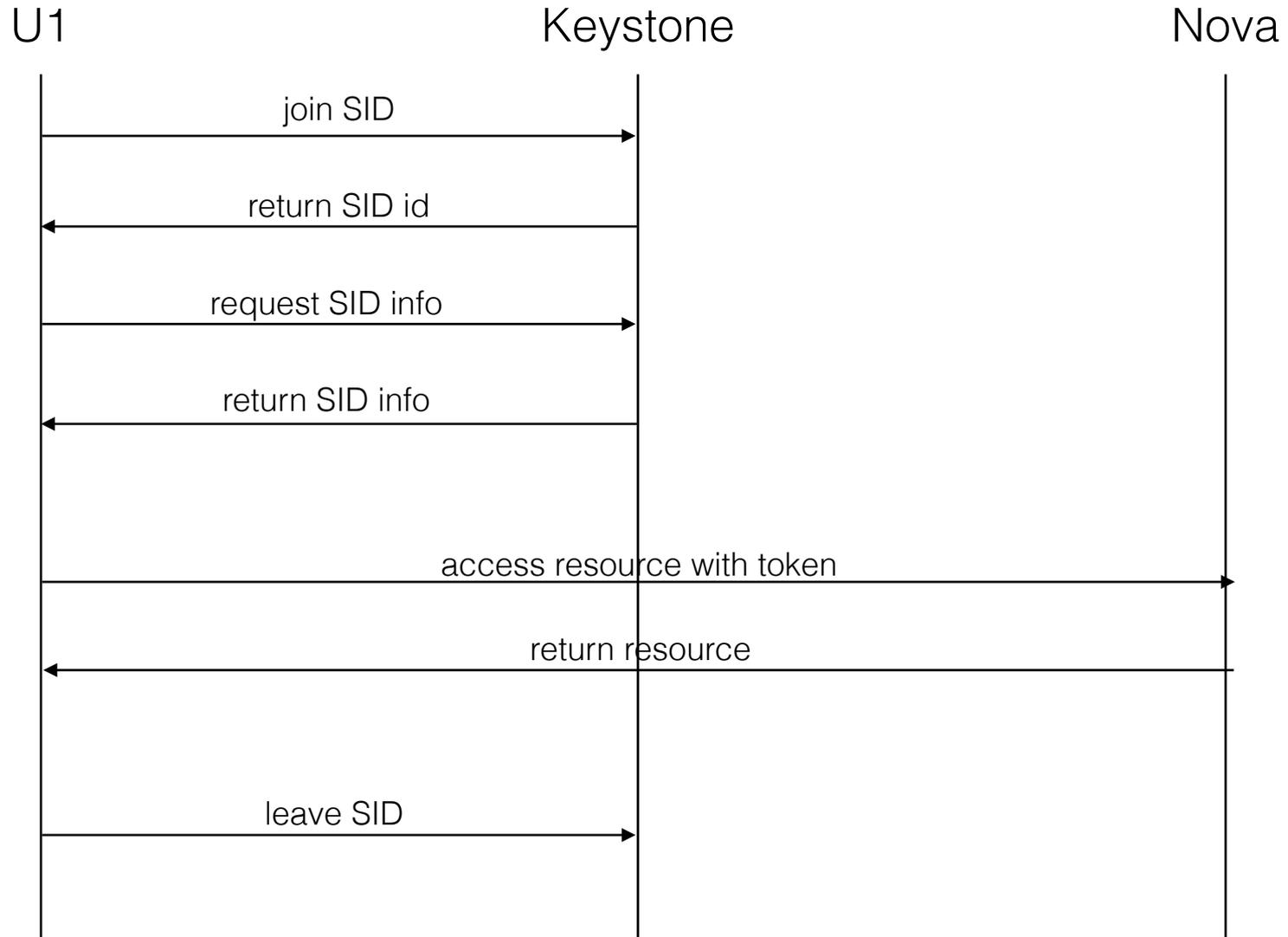
Some Implementation details

➤ Tips:

- ❖ Domain admin create the table for every unique request and map the table according to the request
- ❖ All the members in the group have to send the request to create the group
- ❖ Each time a user requests to leave the group, update the table

SID Table (domain admin)

	U1	U2	U3	U4
SID1	c	m	m	
SID2	m	c		
SID3		c	m	m



➤ Steps:

- ❖ U1 send join_SID request
- ❖ Keystone return SID ID
- ❖ U1 request SID info
 - waiting for U2, U3
 - ready
- ❖ Keystone return SID info
 - shared project name
 - shared swift url
 - user's container url(name)
 - SID member's container url(name)
 - shared container url(name)



Cited from google search.