Small Community Access Right Delegation Protocol

for Grid Enable Infrastructure

Suriya Uruekolan and Vara Varavithya
Department of Electrical Engineering
King Mongkut's Institute
**of Technology North Bangkok**

http://hpc.ee.kmitnb.ac.th

Agenda

- **Grid computing : Virtual Organization**

- **Grid Security Concept**

- **Management and Problem in VO**

- **Related Works :CAS and Akenti**

- **Small Community in VO**

- **Protocol delegation access right and testbed**

- **Conclusion**

Grid Computing : Virtual Organization

- ## VO (Virtual Organization)
  - Abstraction to model distributed resource sharing and allocation across different organizational entities

Organization B

VO 1 run Jobs A

VO 2 run Jobs B
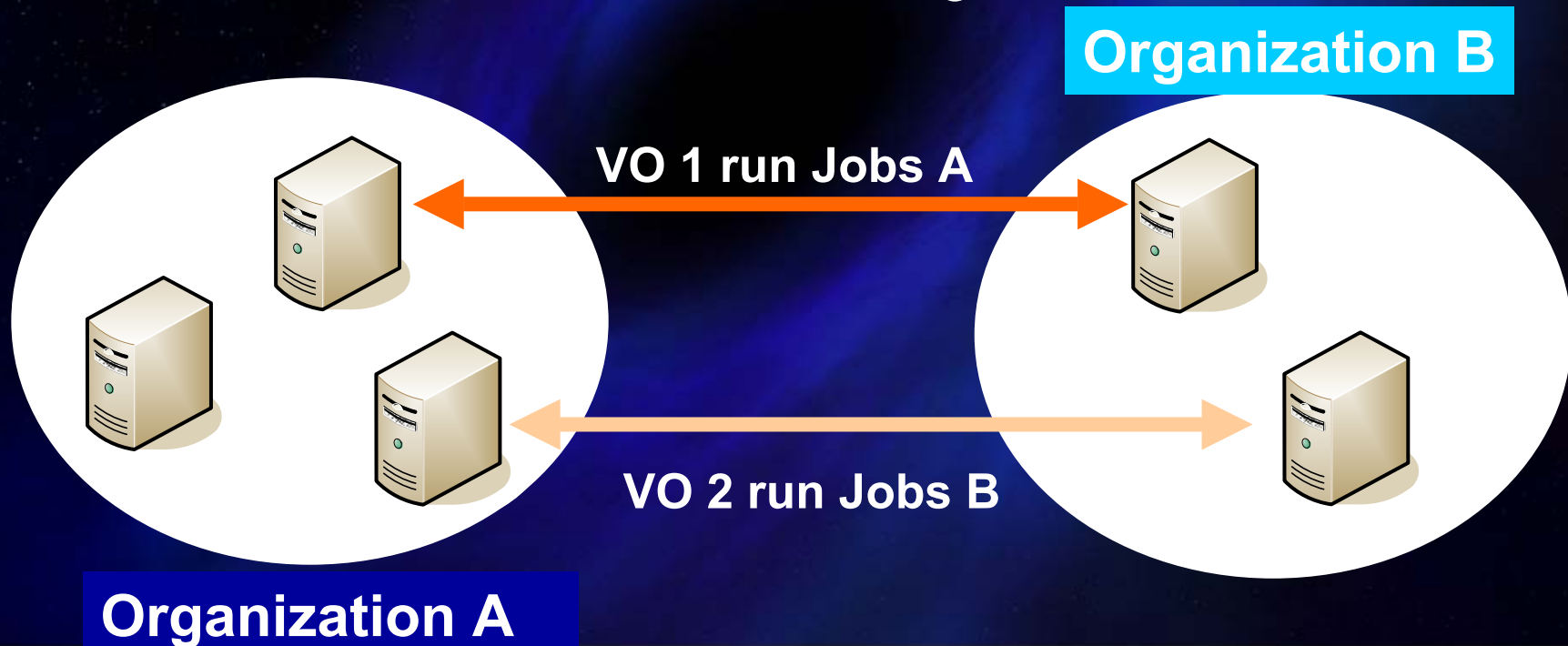
Organization A

Virtual Organization Role

Users

- Large and dynamic population
- Confidential data
- Heterogeneous privileges

Grid

Resources

- Access Patterns
- Local policies
- Membership

Grid Security Properties

- **Authentication**

- **Authorization**

- **Message Protection**

  - **Message Integrity**

  - **Message confidentiality**

- **Single sign-on**

Grid Security Infrastructure

Proxy Certificate

X.509 SSL

Delegation

Two core concepts :

- **X.509 digital certificates used as identity credentials**

- **Proxy Certificate used to delegate identity temporarily to other credentials**

Grid Security : Security VO manage

- **Management of VO**
    - Discover VO by Grid participants
    - Authentication and authorization
    - Access control: Participants access shared resources

- **The problem of VO security**
    - Large number of distributed resources
    - Dynamic and complex relationships among organizations across trust domains
    - Resource utilization scenarios are complex and changing dynamically

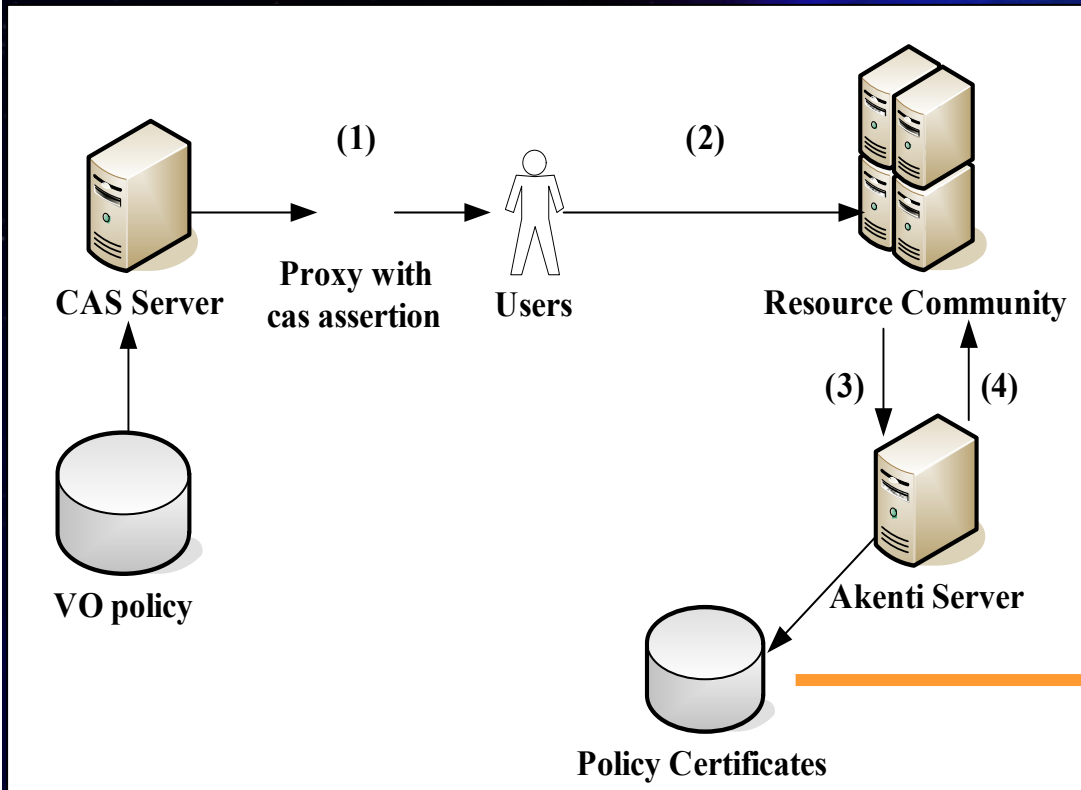# Grid Security : Authorization management

• Community Authorization Service

CAS Server

CA

Request proxy to CAS server

Reply restriced proxy to user
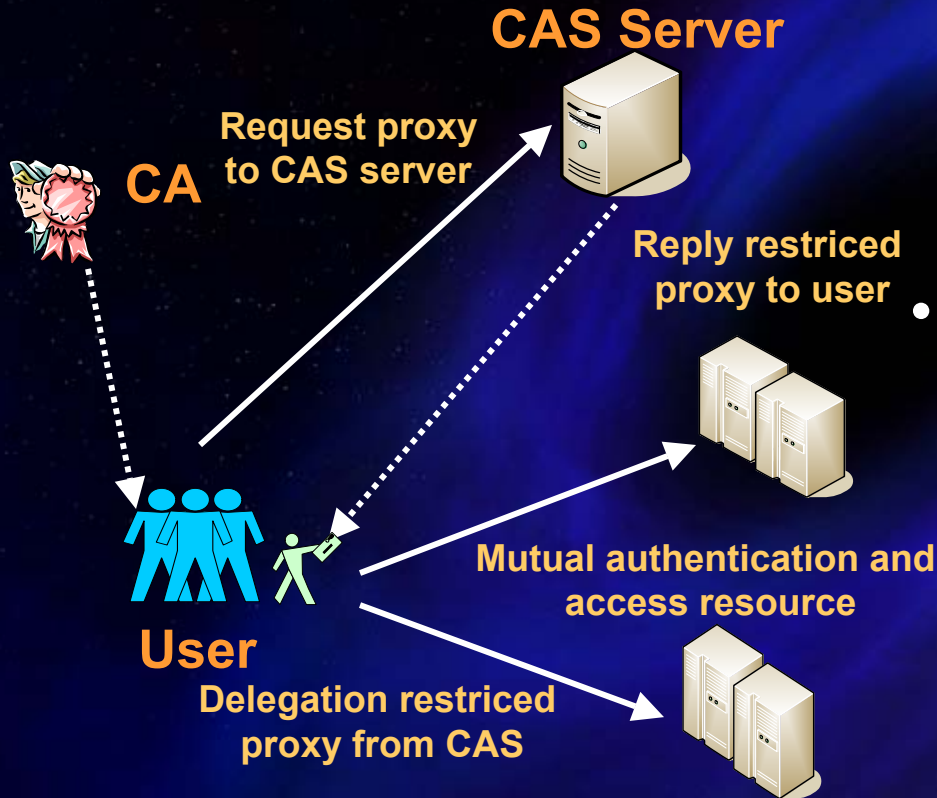
CAS concept:

• Reduce trust relationship by
- Group user to community
- Resource authorized community
- Community authorized user
- Constrain in proxy certificate
- Support GridFTP Service in globus toolkit 2.x-3.x

User

Mutual authentication and access resource

Delegation restriced proxy from CAS

Grid Security : Authorization management

• CAS with Akenti

CAS Server

(1) Proxy with cas assertion

Users

(2)

Resource Community
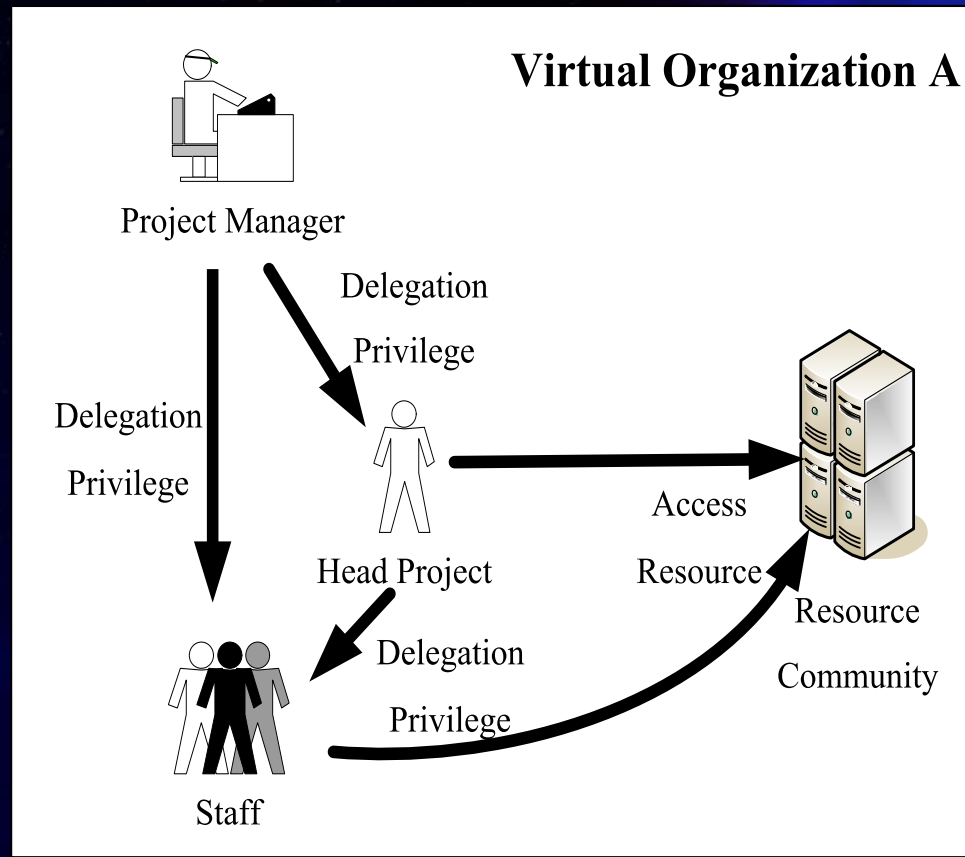
VO policy

(3)   (4)

Akenti Server

Policy Certificates

- Akenti support policy language in XML format

- support GRAM service in globus toolkit

(DN=/O=DOEGrids/OU=People/CN=Jane Doe) ||

(role=developer && (time>5pm) && (time<8am)) ||
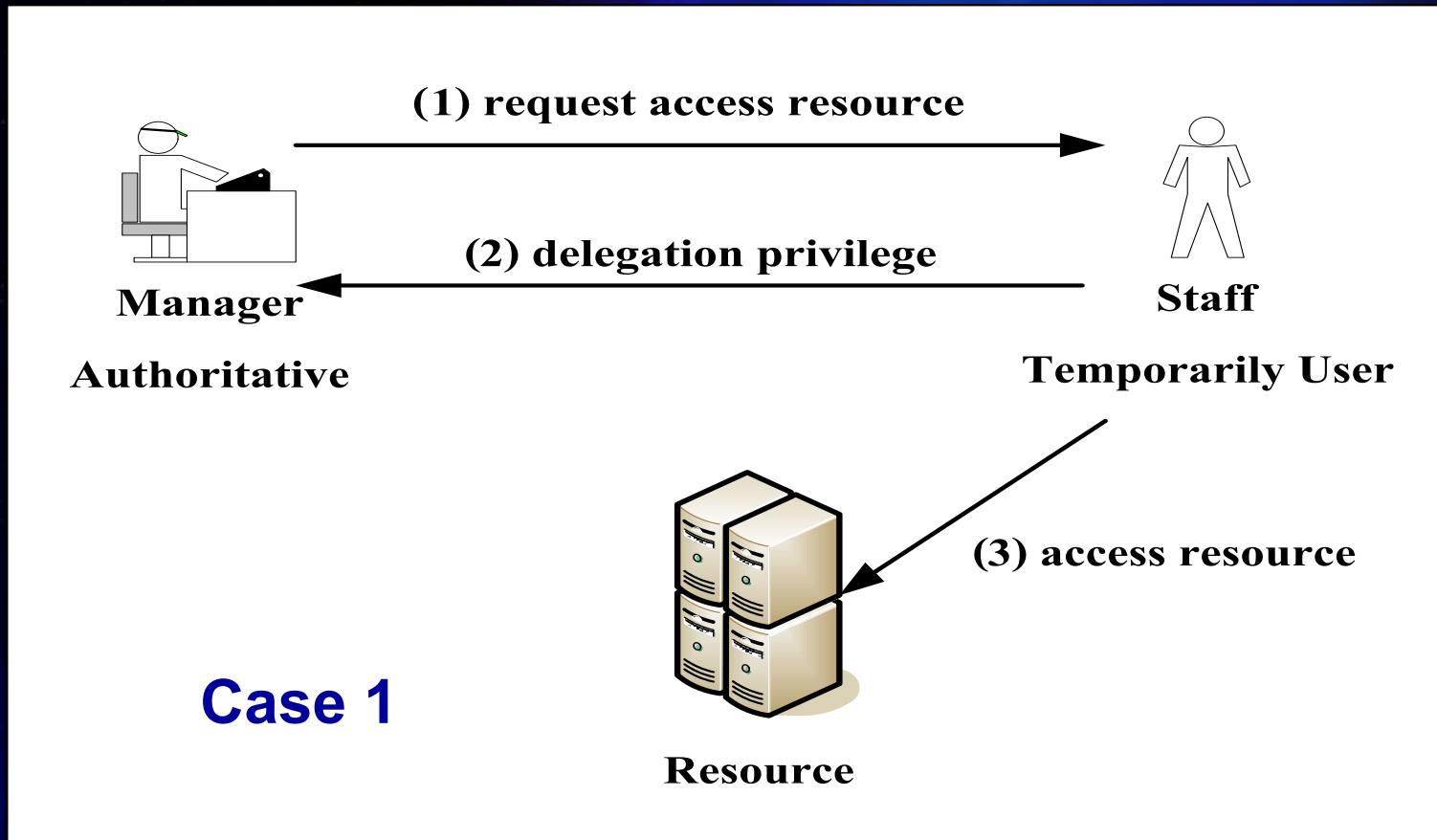
(group=clients && executable=TRANSP)

Actions=start

Grid Security : Small Communities in VO

- ## Component of small communities in VO

Virtual Organization A

Project Manager

Delegation

Privilege

Delegation

Privilege

Head Project

Delegation

Privilege

Staff

Access

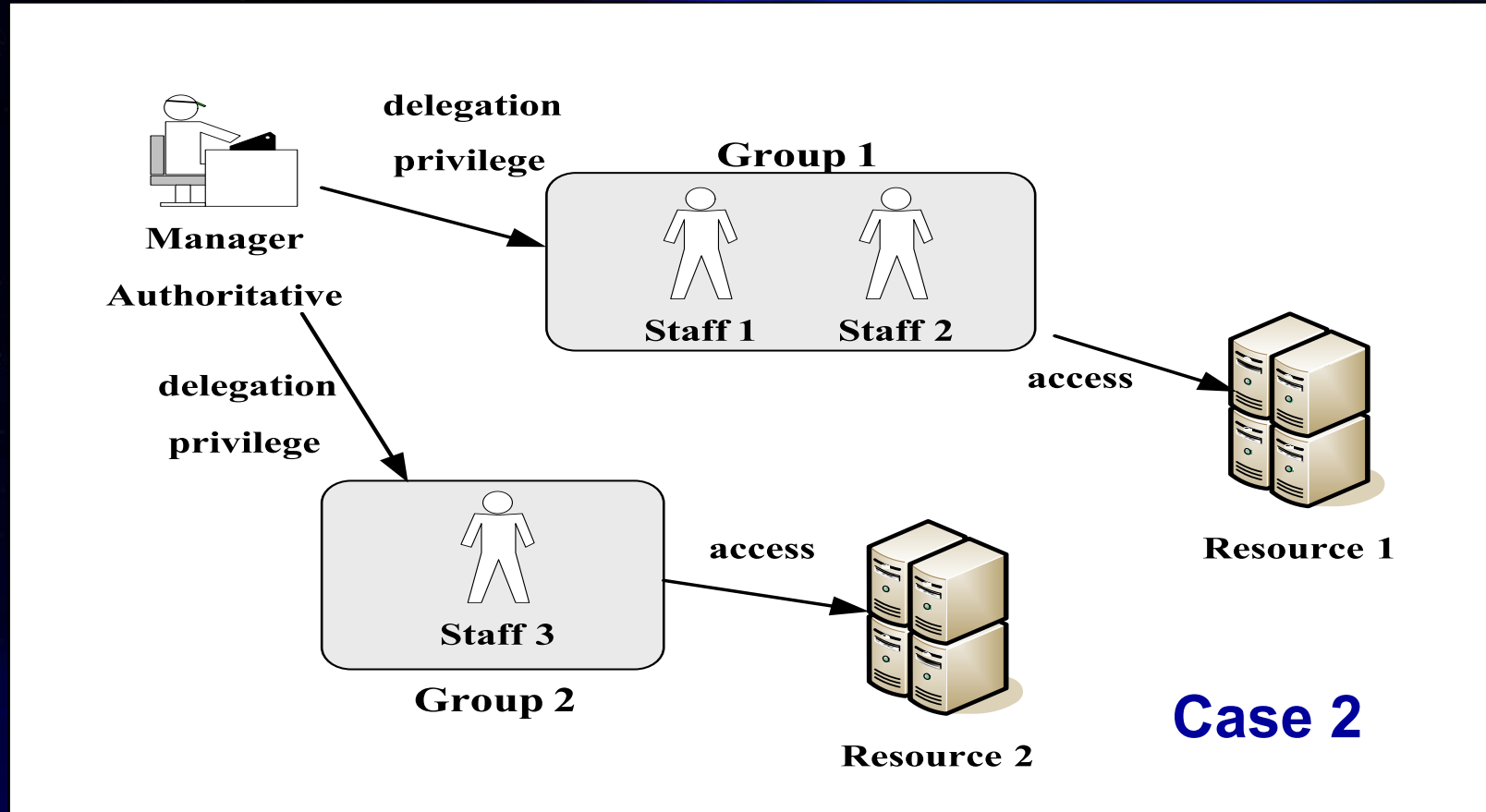Resource

Resource

Community

- **Static users for assign authoritative**
- **Temporarily users accept authoritative from static users**
- **Users operation same jobs in small communities in VO**
- **Multi-level authoritative from user to user**

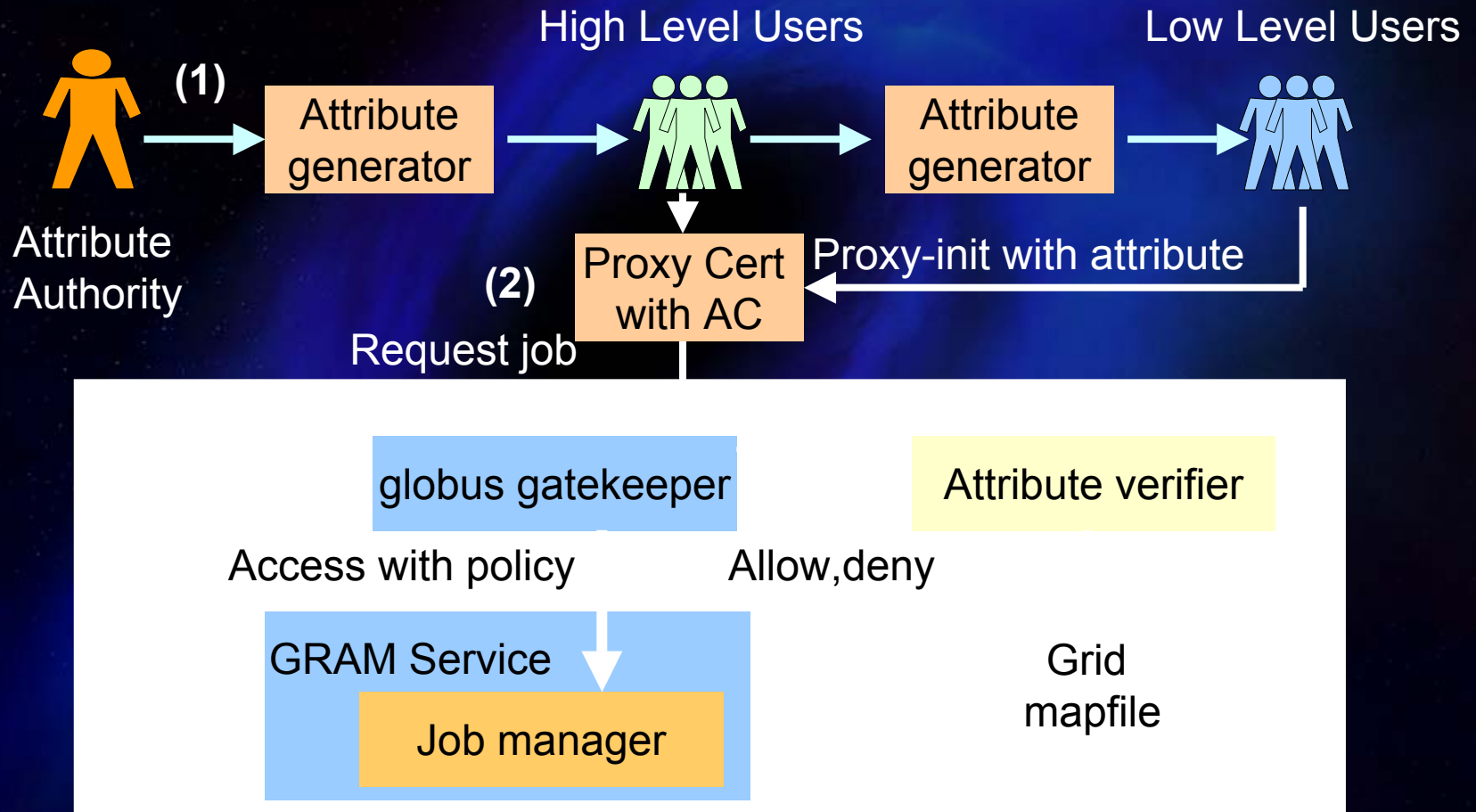# Small Communities in VO: Characteristics

(1) request access resource

(2) delegation privilege

Manager

Authoritative

Staff

Temporarily User

(3) access resource

Case 1

Resource

Small Communities in VO: Characteristics

Small Community Access Right Protocol:

• Architecture

High Level Users

Low Level Users

(1)

Attribute
generator

Attribute
generator

Attribute
Authority

Proxy-init with attribute

(2)

Proxy Cert
with AC

Request job

globus gatekeeper

Attribute verifier

Access with policy

Allow,deny

GRAM Service

Grid
mapfile

Job manager

Attribute Generator Concept

Public Key

Subject:O=Grid, O=ThaiGrid,
OU=ee.kmitnb.ac.th, CN=suriya
Issuer: C=TH, O=Grid, O=ThaiGrid,
CN=ThaiGrid CA
Expiration date: Aug 22 08:08:14 2005
GMTSerial number: 625 (0x271)

Attribute Certificate:
Issuer : O=Grid, O=ThaiGrid,
OU=ee.kmitnb.ac.th, CN=suriya
Holder : O=Grid, O=ThaiGrid,
OU=ee.kmitnb.ac.th, CN=gridstaff
Validity date : Jan 22 08:08:14 2005 GMTSerial
extension : sun.ee.kmitnb.ac.th/allow
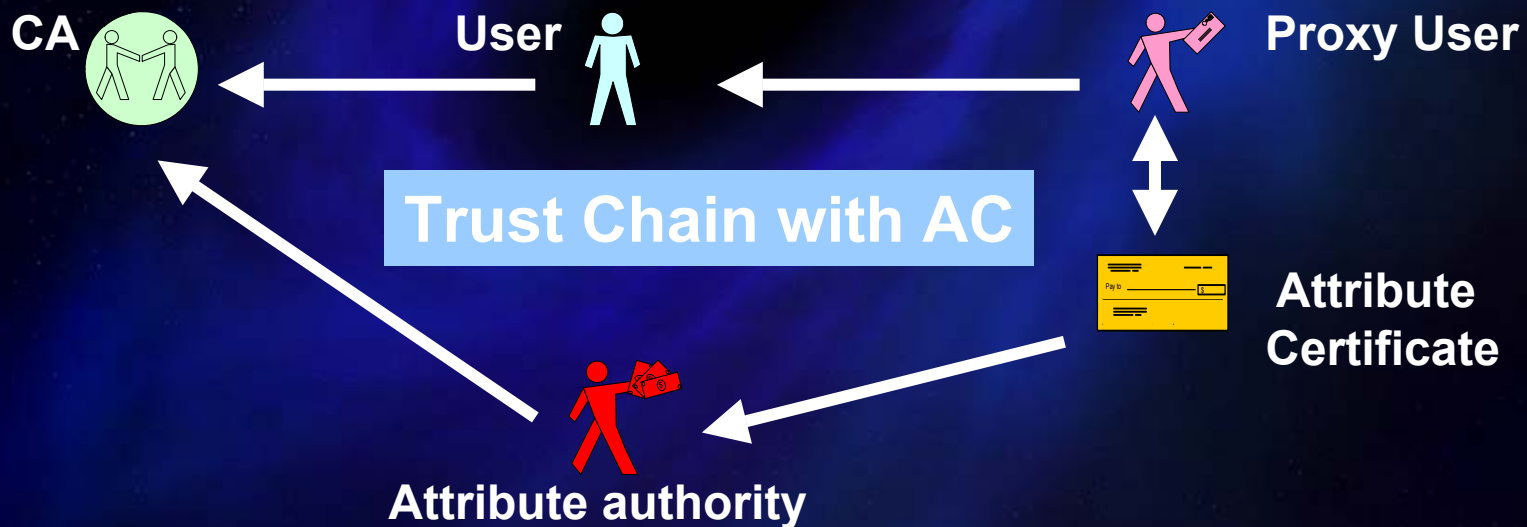Issuer Signature : MD5RSAEncryption

CA Digital signature

Concept :

- **Use Attribute Certificate concept for assign privilege authoritative**

- **Embed Attribute Certificate into X.509 Certificate**
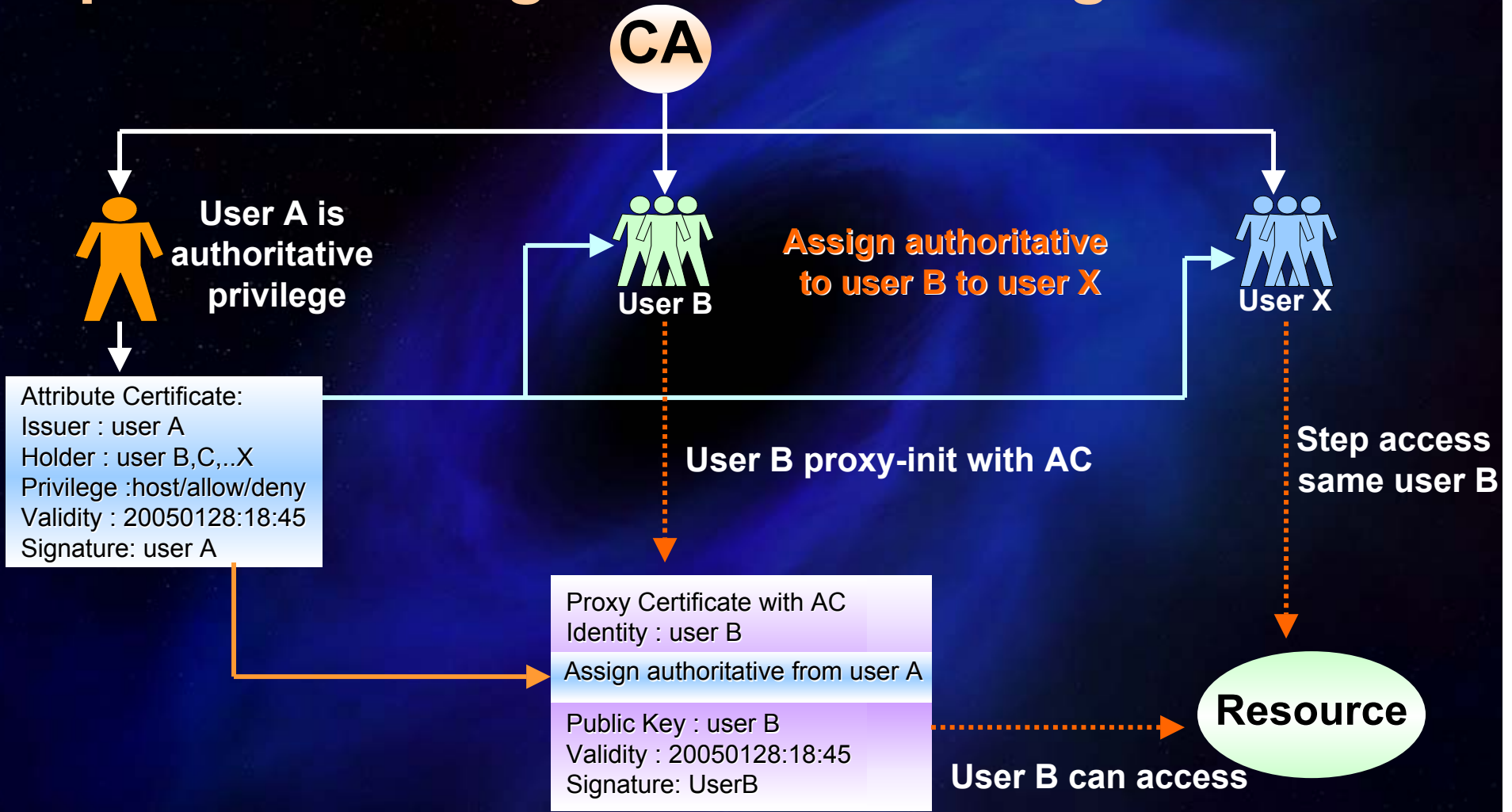
Attribute Verifier :Concept

- **Verify Policy in attribute certificate and control policy to access GRAM service**

gram: // sun.ee.kmitnb.ac.th / allow

| Grid service privilege | hostname | Policy action |
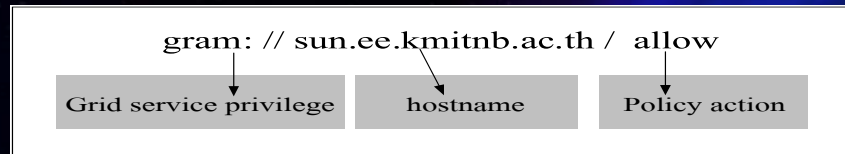
- **Chain of trust with attribute authority**

CA

User

Proxy User

Trust Chain with AC

Attribute Certificate

Attribute authority

Delegation Access Right Protocol: Testbed

Attribute Authority	User Access with AC	Host Authen& Authorization	GRAM Service
suriya	gridstaff	PALM Cluster	Allow GRAM
	gridstaff	EnQueue Cluster	Deny GRAM

```
[gridstaff@sun bin]$ ./tgpac-proxy-init -ac ../../gridstaff.pem
***                                          ***
***              Welcome to the IAIK JCE Library              ***
***                                          ***
Your identity: CN=gridstaff,OU=ee.kmitnb.ac.th,OU=ThaiGrid,O=Grid
Your AC: Version: 2
Holder: {entityName: directoryName: C=,O=Grid,OU=ThaiGrid,OU=ee.kmitnb.ac.th,CN=gridstaff,EMAIL=}
Issuer: {directoryName: CN=Suriya Urueakolan,OU=ee.kmitnb.ac.th,OU=ThaiGrid,O=Grid}
Signature algorithm: md5WithRSAEncryption(1.2.840.113549.1.1.4)
Serial number: 5
Valid not before time: Thu Dec 09 11:01:58 ICT 2004
Valid not after  time: Sat Dec 11 11:01:58 ICT 2004
Attributes: 1

Certificate Fingerprint(MD5)  : 37:F0:41:46:6F:8B:97:98:E1:A2:43:82:F5:85:70:59
Certificate Fingerprint(SHA-1): 37:F0:41:46:6F:8B:97:98:E1:A2:43:82:F5:85:70:59

Including AC Issuer Certificate for: CN=Suriya Urueakolan,OU=ee.kmitnb.ac.th,OU=ThaiGrid,O=Grid
Enter GRID pass phrase for this identity: 123456
Creating proxy, please wait...
Adding AC as extension...
Adding AC issuer cert as extension...
Your proxy is valid until Wed Mar16 01:27:00 ICT 2005
[gridstaff@sun bin]$ globus-job-run sun.ee.kmitnb.ac.th -np 1 ./cpi
pi is approximately 3.1416009869231254 , Error is 0.0000083333333323
wall clock time = 0.000104
Process 0 on sun.ee.kmitnb.ac.th
```

Allow access GRAM

```
[gridstaff@sun bin]$ ./tgpac-proxy-init -ac ../../gridstaff.pem
***                                        ***
***            Welcome to the IAIK JCE Library            ***
***                                        ***
Your identity: CN=gridstaff,OU=ee.kmitnb.ac.th,OU=ThaiGrid,O=Grid
Your AC: Version: 2
Holder: {entityName: directoryName: C=,O=Grid,OU=ThaiGrid,OU=ee.kmitnb.ac.th,CN=gridstaff,EMAIL=}
Issuer: {directoryName: CN=Suriya Urueakolan,OU=ee.kmitnb.ac.th,OU=ThaiGrid,O=Grid}
Signature algorithm: md5WithRSAEncryption (1.2.840.113549.1.1.4)
Serial number: 5
Valid not before time: Thu Dec 09 11:01:58 ICT 2004
Valid not after  time: Sat Dec 11 11:01:58 ICT 2004
Attributes: 1

Certificate Fingerprint(MD5)  : 37:F0:41:46:6F:8B:97:98:E1:A2:43:82:F5:85:70:59
Certificate Fingerprint(SHA-1): 37:F0:41:46:6F:8B:97:98:E1:A2:43:82:F5:85:70:59

Including AC Issuer Certificate for CN=Suriya Urueakolan,OU=ee.kmitnb.ac.th,OU=ThaiGrid,O=Grid
Enter GRID pass phrase for this identity 123456
Creating proxy, please wait...
Adding AC as extension...
Adding AC issuer cert as extension ...
Your proxy is valid until Wed Mar16 02:11:02 ICT 2005
[gridstaff@sun bin]$ globus-job-run algorithm.ee.kmitnb.ac.th -np 1 ./cpi
GRAM Job submission failed because the connection to the server failed
```

deny access GRAM

Conclusion

- **Build tool support delegation access right protocol for small communities in VO**

- **Modify Proxy Certificate by embed Attribute Certificate for access rights**

- **Decrease administrative for add grid-mapfile and account local for temporarily grid user**

- **Delegation access right protocol in small community support GRAM service in globus tookit 2.x**