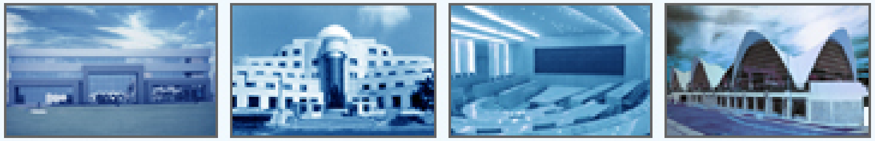
Infosys®

POWERED BY INTELLECT
DRIVEN BY VALUES

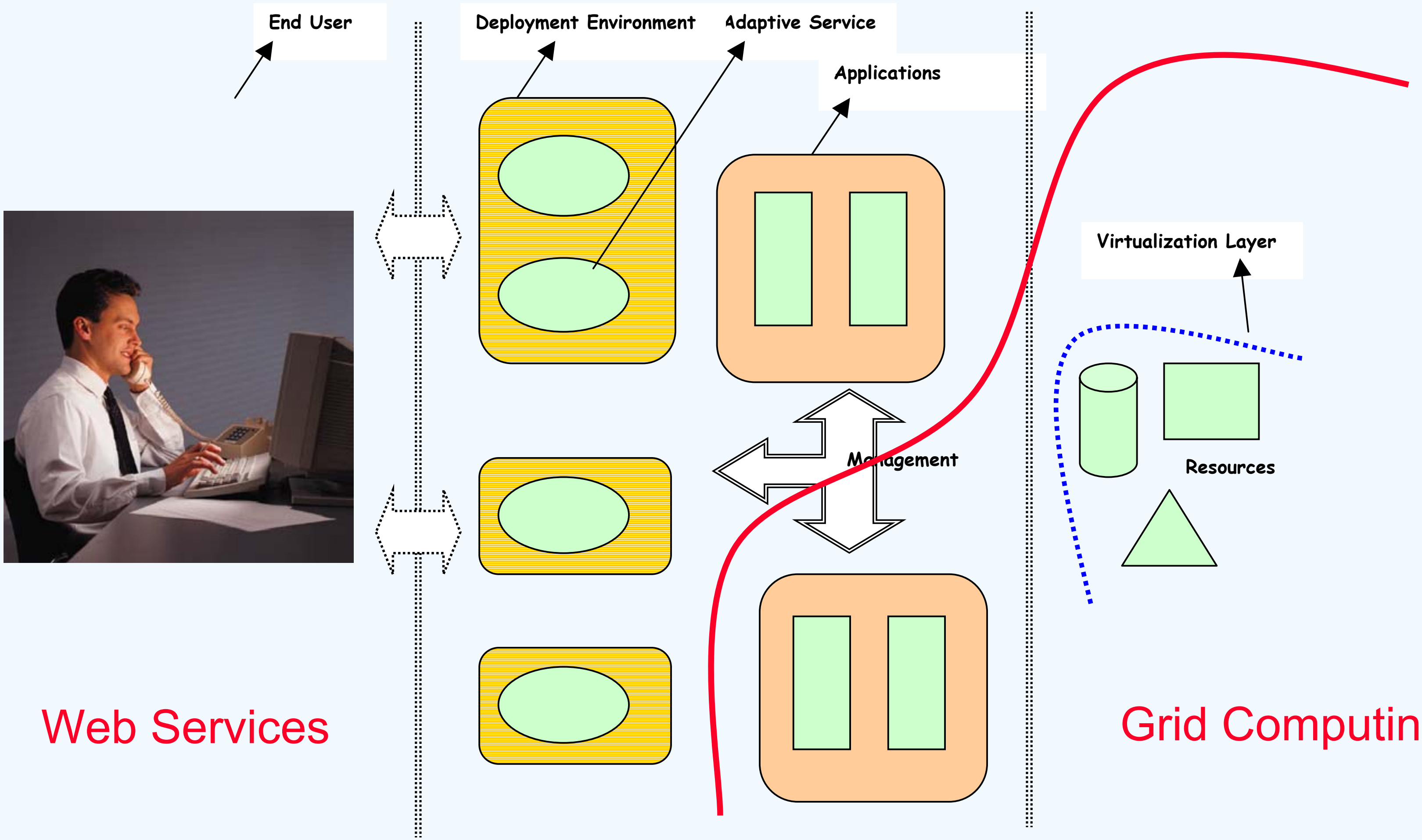


Virtualized Credential & Policy Manager

Anirban Chakrabarti

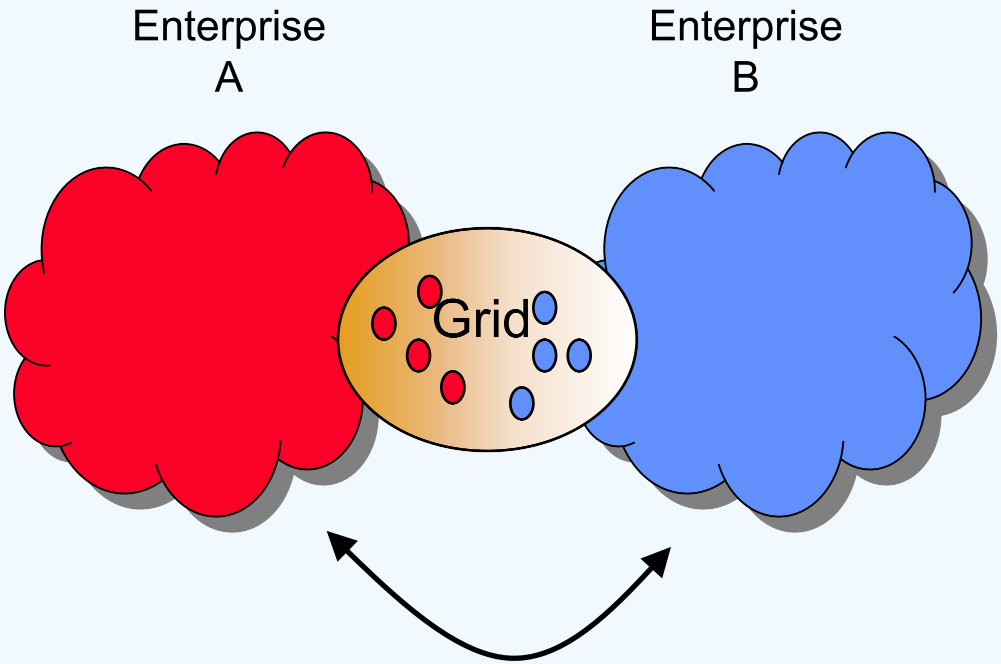
SETLabs, Infosys Technologies

Shared Service Model



Collaborative Grid

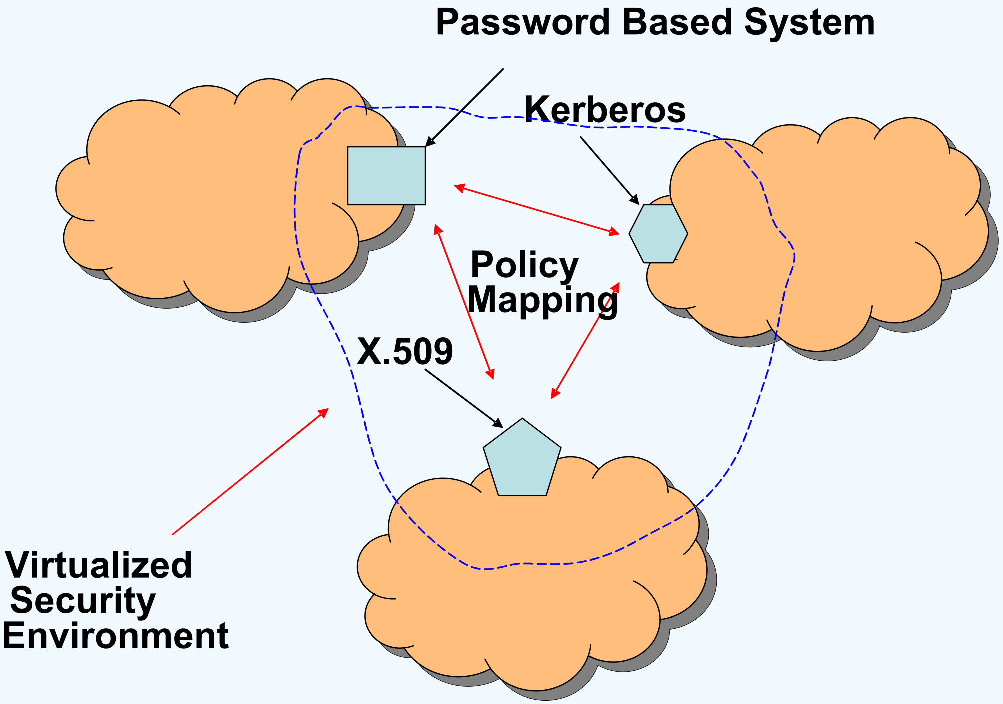
- In a collaborative environment
  - Grid resources need to be shared
  - Policies need to be shared and understood
    - Need a policy exchange infrastructure
    - Need to trust each other
    - Need to have a shared security infrastructure
  - Collaboration across enterprises



Seamless sharing of resources

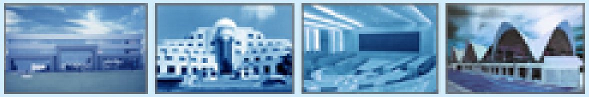
True Virtualization – Inter-domain View

- In a collaborative environment
  - Grid resources need to be shared
  - Policies need to be exchanged
    - Need a common policy exchange language
  - Collaboration across enterprises
- Virtualized Credential Manager (VCMan) is a solution

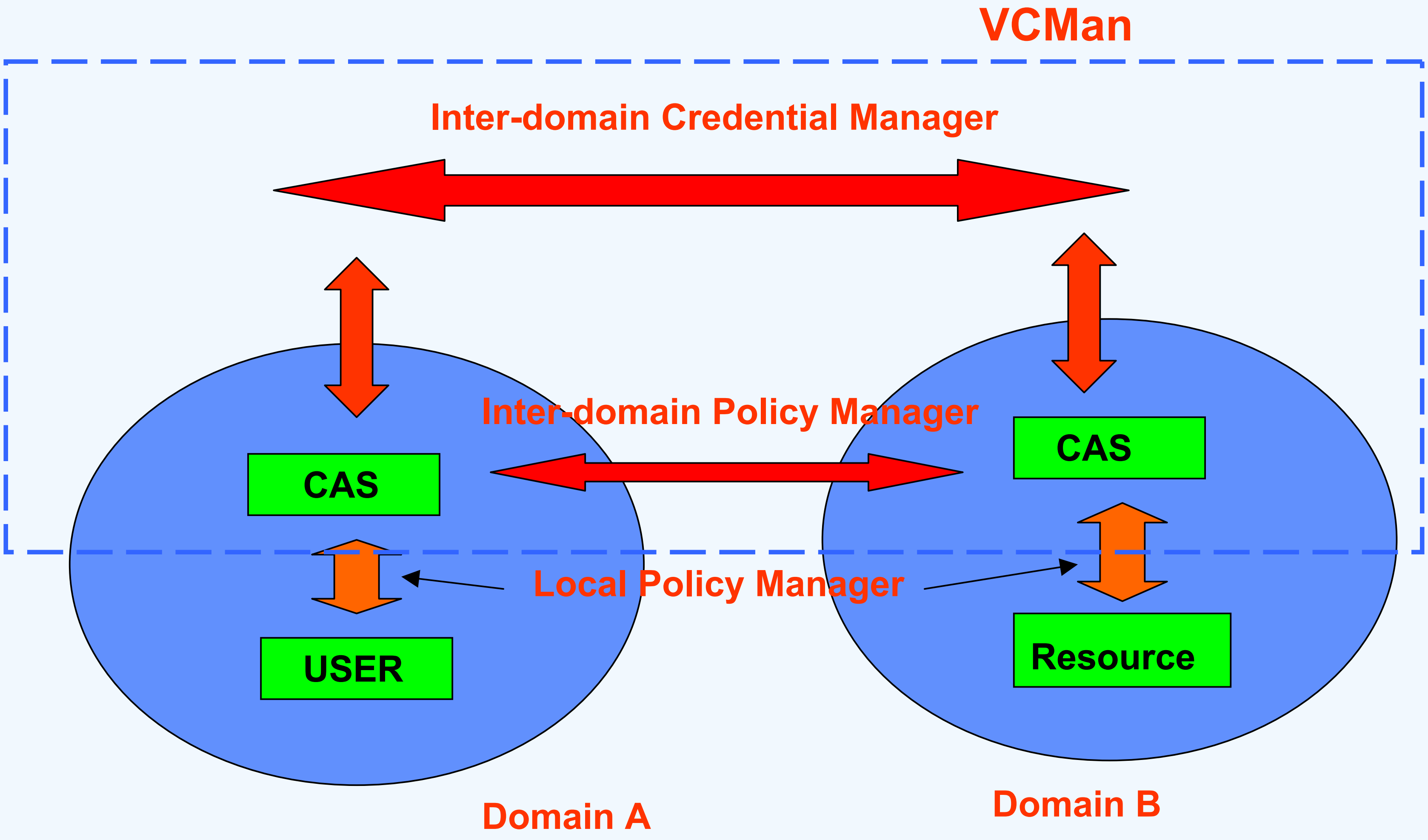


Virtualized Credential and Policy Manager (VCMan)

- VCMan virtualizes the policy management across different domains
  - Enables a mechanism to expose domain policies
    - Through a XML based language called PXLang
  - Policies can be exchanged between domains
    - Through Local Policy Manager (LPM) and Inter-domain Policy Manager (IPM)
  - Enables users to submit jobs to remote domains
    - Uses Community Authorization Service (CAS) for creating domain assertions
  - Enables credential management
    - Through remote execution of jobs
    - Domains having different authentication systems

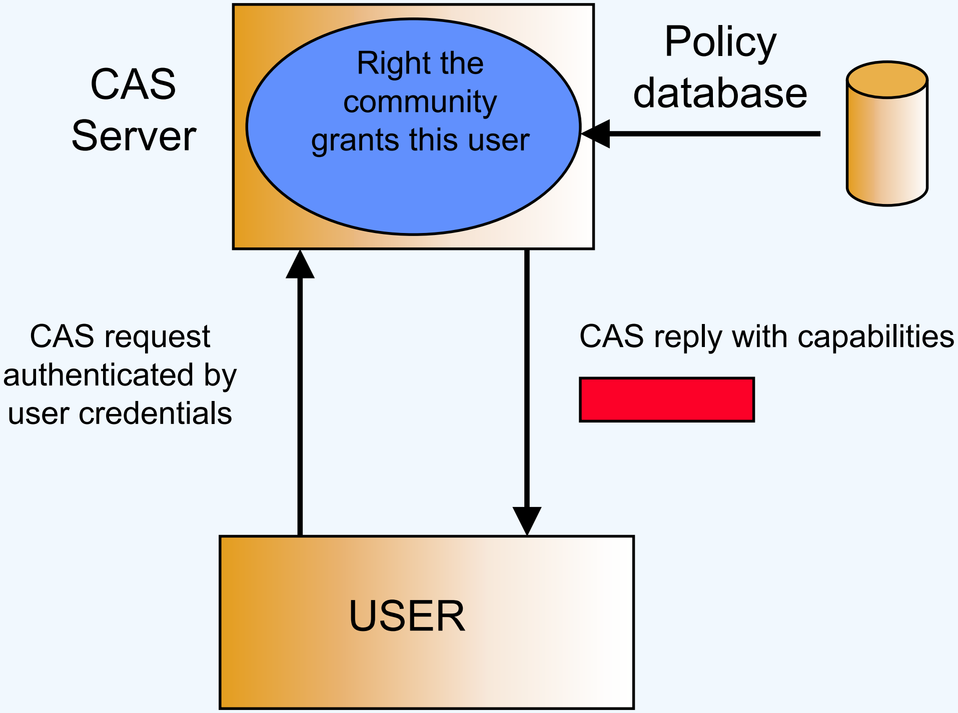


VCMan Architecture



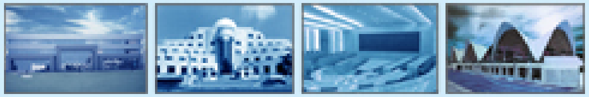
Local Policy Manager (LPMan)

- Mapping the policies within a domain
- Is carried out through Community Authorization Service (CAS)

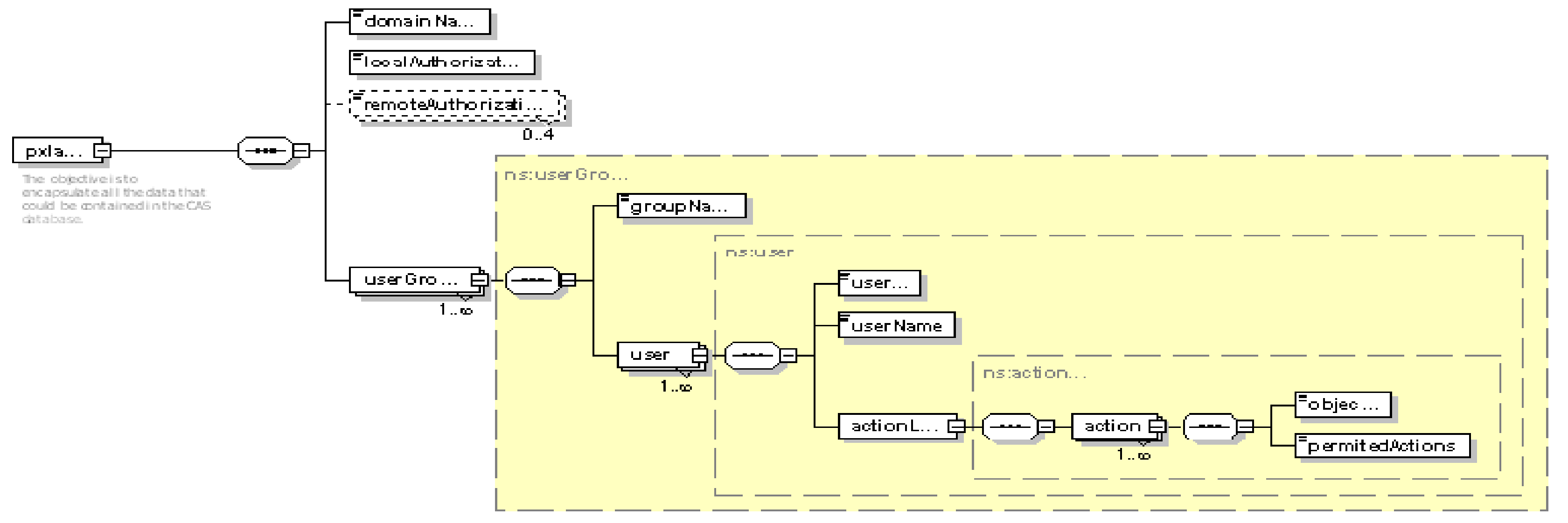

CAS Server
Right the community grants this user
Policy database
CAS request authenticated by user credentials
CAS reply with capabilities
USER

Inter-domain Policy Manager (IPMan)

- Inter-domain Policy Exchange
  - Development of a CAS policy description language (PXLang)
    - Describes the policies in a XML based language
    - Derived from WS-Policy
  - Domain Directory Service
    - Assigns jobs to specific domains
- Inter-domain Job Execution
    - Execution of job in a different domain
    - Management of jobs based on policies



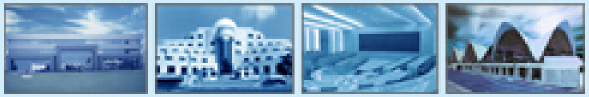
Policy Exchange Language



- XML based markup language.
- Capable of capturing all the data required for cross domain policy mapping from the CAS database.
- Validating Schema
- Actions permitted on objects modeled on the UNIX file system permissions.

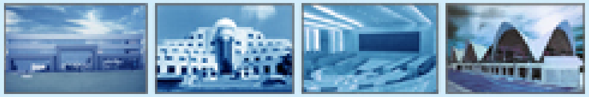
Directory Service

- Provides a single query able interface that provides
  - A Lists of all the different CAS that constitute to form the grid
  - CAS name to machine name lookup
- Easy to maintain and Update
- Provided as a grid service
  - Used by the CAS for domain lookup

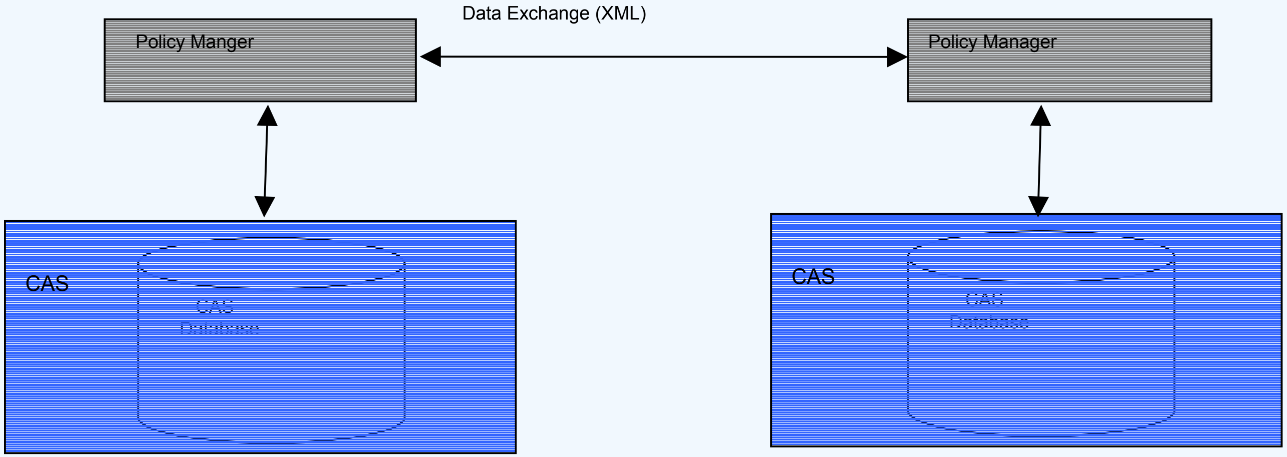


Inter domain Policy Exchange

- When a job is submitted to be executed in another domain
  - Domain information is obtained from the directory service
  - Information is needed whether the job can be executed in the domain
    - Policy is exchanged between the domains
    - Through a grid service
- The policy is maintained as a soft state
  - Expires
    - If it is not accessed for a certain amount of time



Inter-domain Policy Exchange

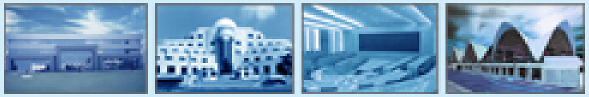


Cross Domain Policy Exchange

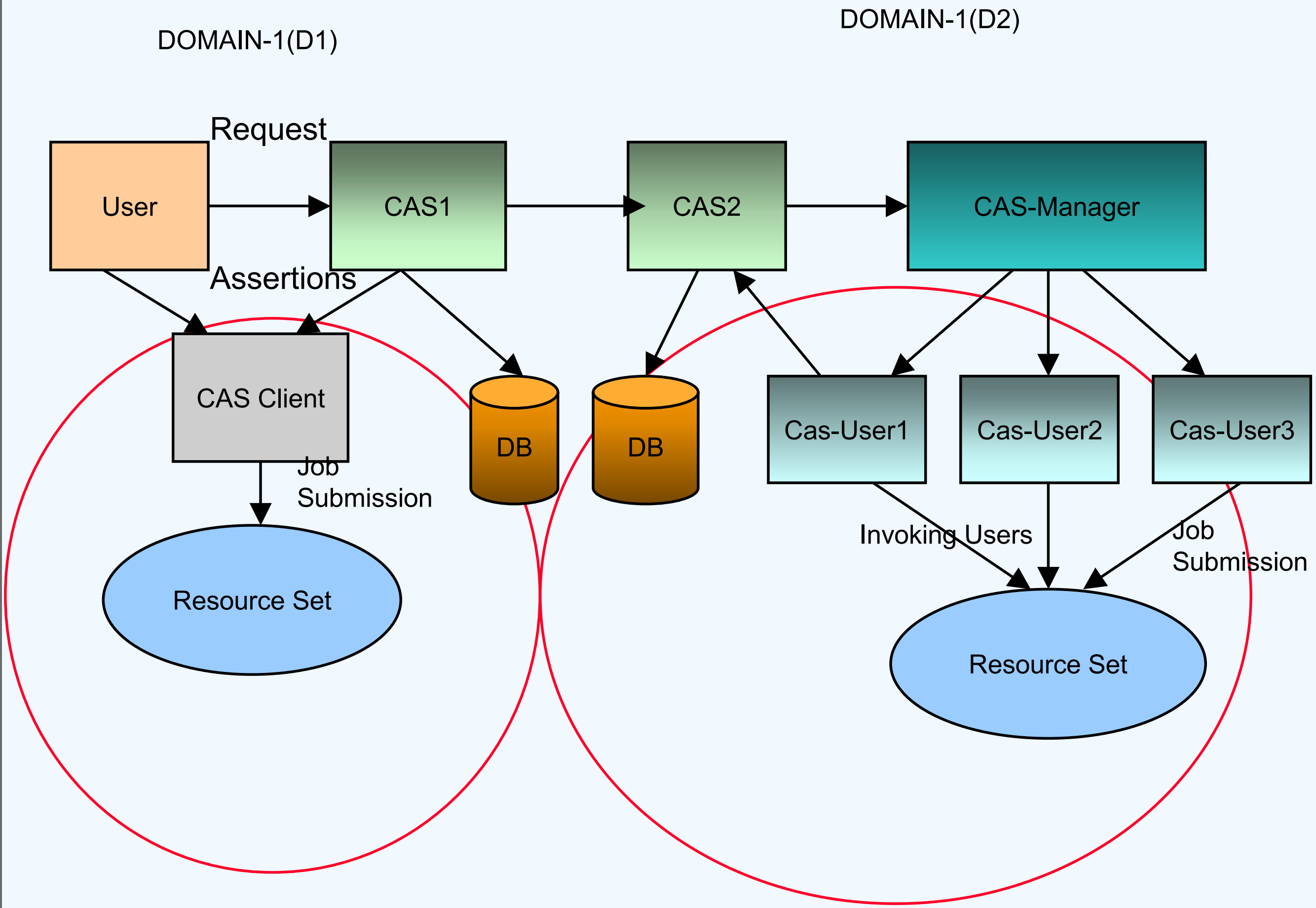
- Extends the capability of CAS to manage policies across domains.
- Data exchanged across domains through custom defined markup language Pxlang
- Pxlang capable of encapsulating all the data contained in a the CAS database.

Inter Domain Job Execution

- When a job is submitted to the local domain
  - CAS assertions is obtained
  - Job is submitted to the local resource
- When a job is submitted to a remote domain
  - Directory server is called to get the domain information
  - Job submission manager (JSM) becomes a user in the other domain
    - There may be multiple users based on user groups
    - JSM resides in the CAS server
  - JSM submits to the JSM of the remote domain as the correct user
    - After checking the credentials for the user
  - Remote JSM
    - Does some credential checks
    - Submits the job to the resources



Inter Domain Job Execution



- Scenario – A user of domain-1(D1) needs to submit a job to the resource of domain-2(D2).

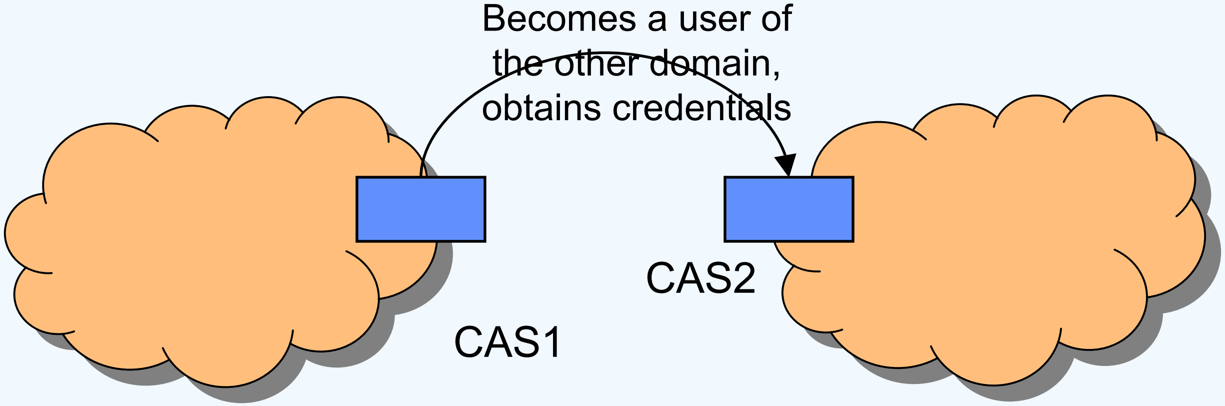
- The user first produces his certificate to CAS server of D1. Based on the domain information, the CAS server checks the directory server and then re-directs the request to the CAS server of D2.

- The CAS-Manager is implemented that handles multiple user-requests.

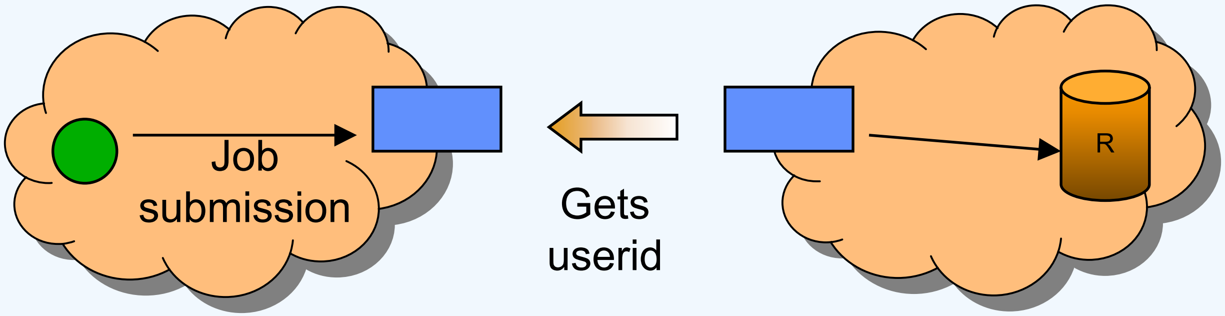
- The CAS-Manager creates different users, which then submit the jobs to the resources.

Inter-domain Credential Manager

- Managing of credentials across domains
  - Different domains have different authentication systems
  - The information is obtained from the PXLang
    - Through a grid service interface

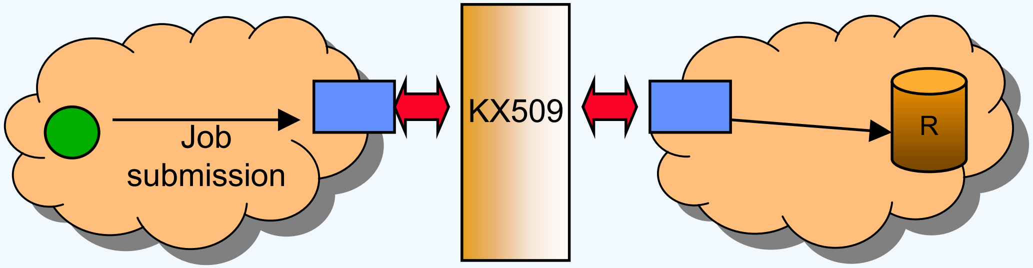


X.509 and Password – A Case Study



- User submits a job to the other domain
  - It presents its X.509 credentials
  - Checked by the JSM
- JSM gets the user id from the other domain
  - Only the JSM gets one, other users do not need user ids

X.509 and Kerberos – A Case Study



- User submits a job to the other domain
  - It presents its X.509 credentials
  - Checked by the JSM
- KX509 is used to map between X.509 and kerberos credentials
  - Jobs are submitted by the other JSM
- Kx509 is a standalone client program
  - Acquires a short term X.509 certificate (junk Key) from the KCA.
- Certificate and the private key generated by Kx509
  - Are stored in the same cache alongside the Kerberos credentials
  - Eliminates the additional overhead of securely storing long term X.509 credentials

Conclusions & Future Work

- Inter-domain Credential and Policy exchange
  - Important issue in grid computing’s long term virtualization dreams
  - Important in an inter-enterprise environment
- VCMan is a solution
  - Based on Community Authorization Service
- Future Work includes
  - Solution is currently under development
    - Solution will be provided to the globus community
  - Integration of VCMan with VOMS, Akenti