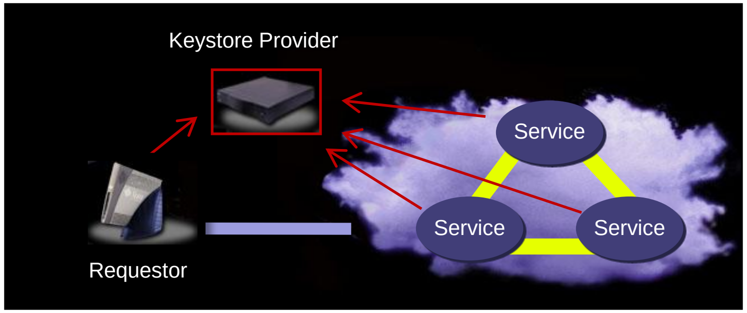
Federated Key Management in Service Oriented Environments

Jennie Mellado

Problem Statement

- File-based storage of large amount of keys does not provide efficient access control in a metacomputing environment.
- Having large number of key files and large number of passwords to access keystore files and keys becomes unmanageable in large S2S environments.
- Inefficient local management of large number of public keys by each service provider collaborating with large number of other service providers.
- When keystore files become not available the security cannot be reinforced.



Managing keys using Java Keystore in Service Oriented Environments does not scale. Replicated central keystore services that are shared among all requestors are needed in metacomputing environments.

Objective

A Scalable Key Management Framework (SKEMAF) for centrally managed and replicated keys in metacomputing environments.

Approach

- Review Literature
  - Key storage and usage
  - Keystore in Client/Service and Peer-to-Peer environments
- Define requirements for SKEMAF
- Analyze data structures and storages representation for central SKEMAF
- Develop SKEMAF methodology
- Design SKEMAF and corresponding model
- Implement and deploy SKEMAF
- Verify and Validate SKEMAF

Schedule

Literature Review Report	October 10, 2007
Requirements for SKEMAF - UML Diagram	October 31, 2007
SKEMAF Methodology - Use Cases and Architecture	November 15, 2007
SKEMAF UML Component Diagram	November 30, 2007
Proposal Presentation	December 2007
SKEMAF Implementation	February 2007
User Agent for Managing Providers Keys	March 2007
Verification and Validation of SKEMAF	April 2007
Thesis Defense	June 30, 2008

Benefits

- Uniform and centralized creation and verification of digital signatures.
- Scalable and reliable federated key management system by replicated central storage.
- Simplified, flexible and efficient management of keys by central keystore services.
- Friendly and intuitive user interface to create and manage keys.
- Keystore maybe used as certificate authority.