Grid Security
: Authentication and Authorization

IFIP Workshop – 2/7/05

Jong Kim

Dept. of Computer Sci. and Eng.

Pohang Univ. of Sci. and Tech. (POSTECH)

Contents

- Grid Security
  - Grid Security Challenges
  - Grid Security Requirements
- Current Status of Grid Security
  - Authentication and Delegation
  - Authorization
  - Grid Security Infrastructure (GSI)
  - OGSA
  - Web Services Security
- Things need more study
  - Authentication Interoperability
  - Fine-grained Authorization
- Summary

Grid Security

- Grid Computing
  - Distributed computing infrastructure with a plenty of resources which are heterogeneous and scattered geographically
  - A controlled and coordinated resource sharing and resource use in dynamic, scalable, and distributed virtual organizations (VOs)

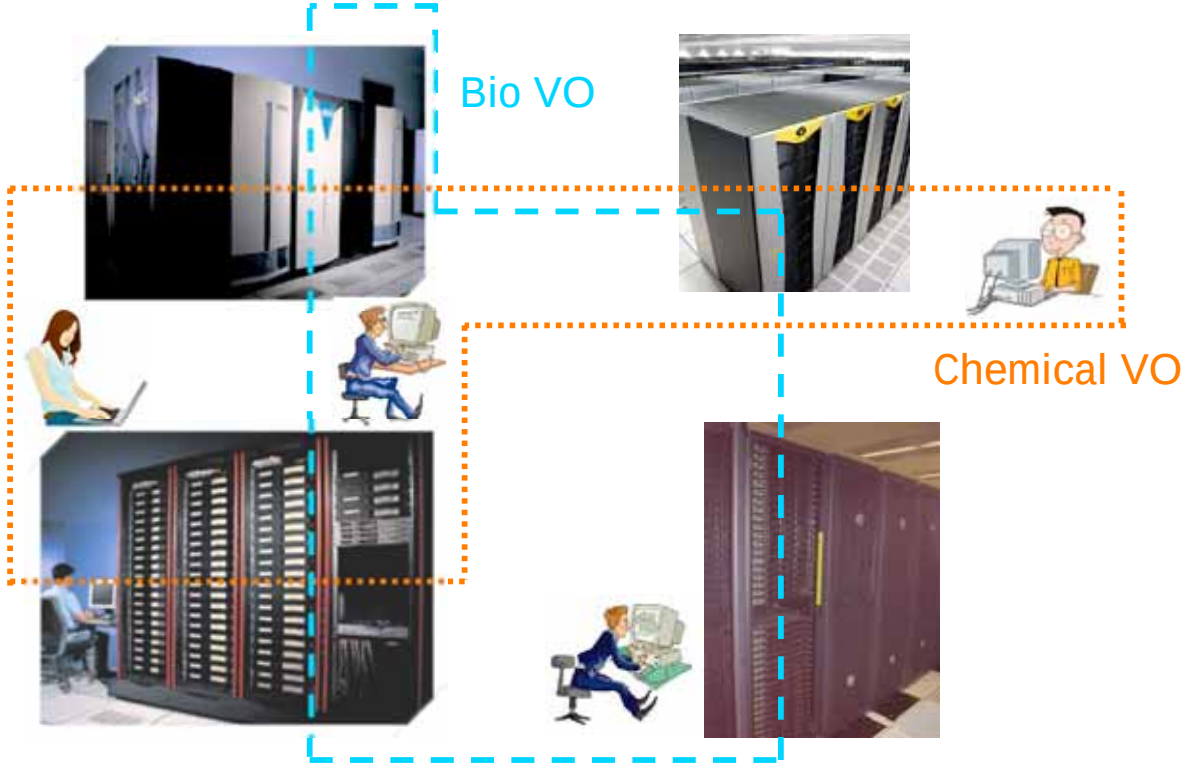
- Security for whom?
  - Resource Providers?
  - Virtual Organization?
  - End-user (participants)?

Grid Security

- What is Grid Security ?
  - Security architecture to enable dynamic, scalable, and distributed VOs protect resources for resource providers, computing entities for VOs, and end-processing for end-users
  - Thru
    - Authentication,
    - Delegation,
    - Authorization,
    - Confidentiality,
    - Privacy, …

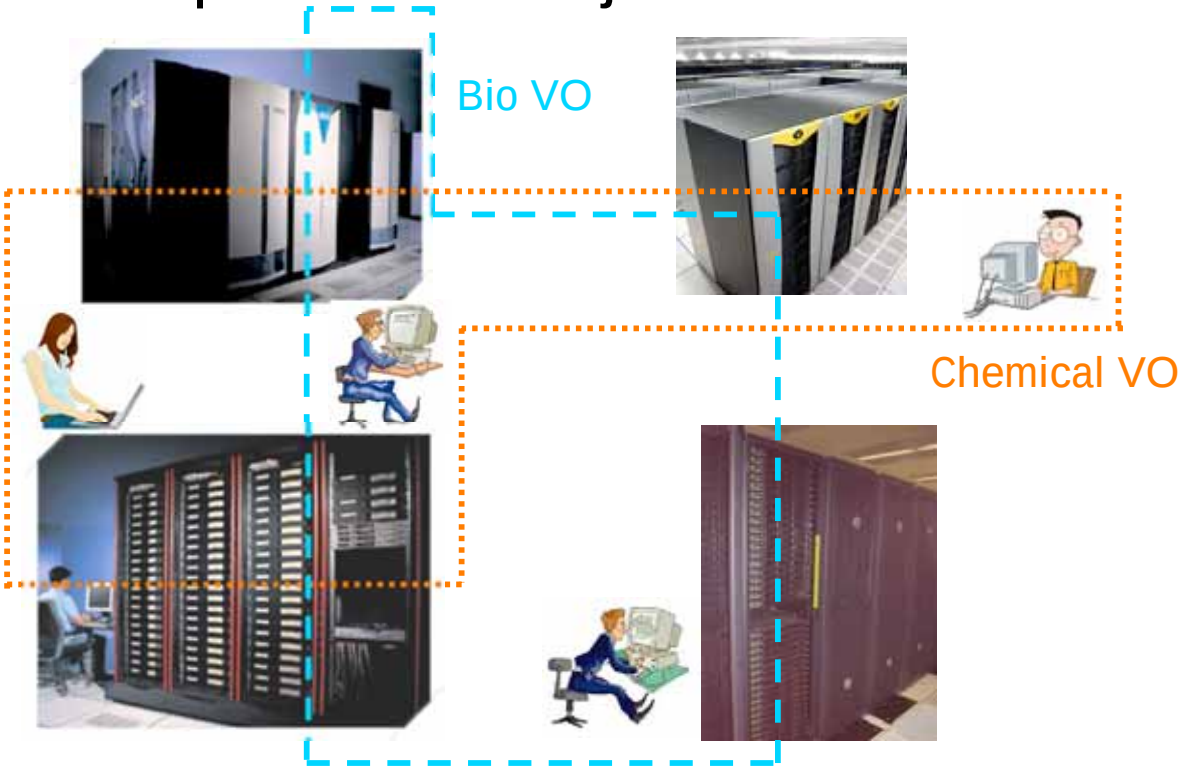
Dynamic VO in the Grid

- Virtual organizations (VOs) are collections of diverse and distributed individuals that seek to share and use diverse resources in a coordinated fashion.
- Users can join into several VOs, while resource providers also partition their resources to several VOs.



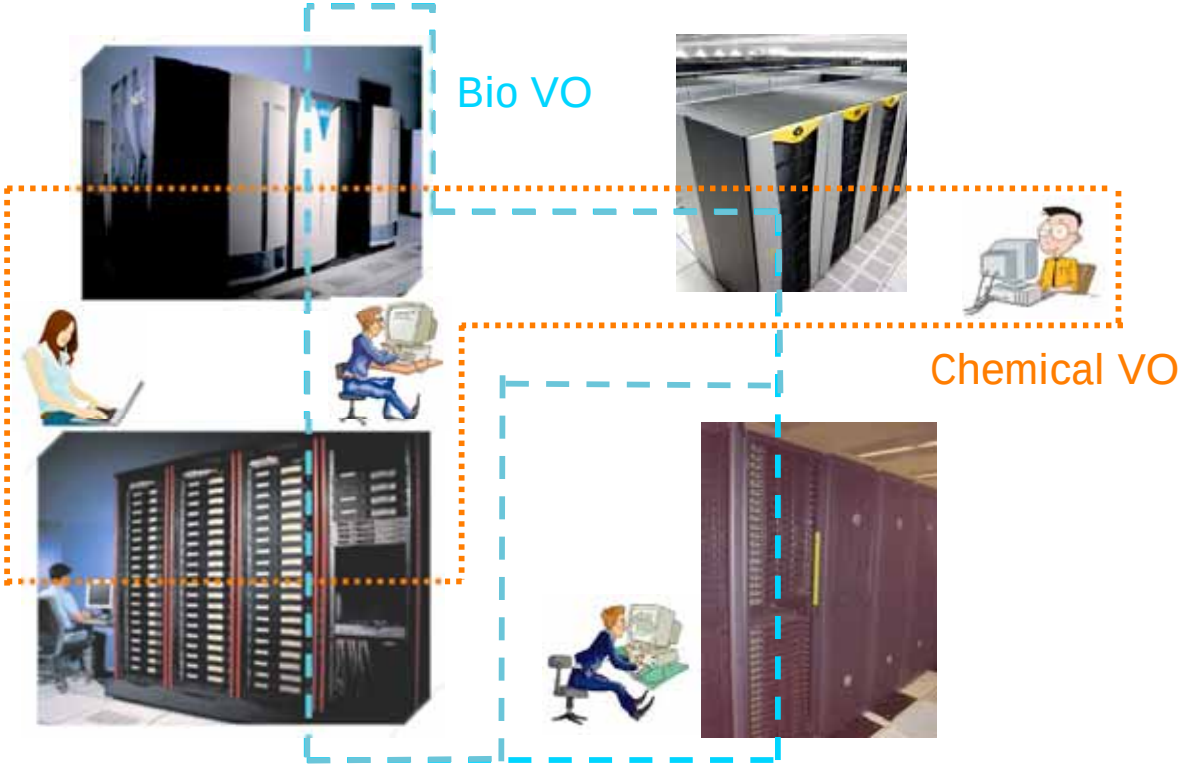
Grid Security Challenges

- Dynamic VO establishment
  - A VO is organized for some goal and disorganized after the goal is achieved.
  - Users can join into or leave VOs.
  - Resource providers can join into or leave VOs.



Grid Security Challenges

- Dynamic policy management
  - Resource providers dynamically change their resources policies.
  - VO managers manage VO users' rights dynamically.



Grid Security Challenges

- Interoperability with different host environments
  - Security services for diverse domains and hosting environments should interact with each other.
  - At the *protocol* level, messages can be exchanged.
  - At the *policy* level, each entity can specify its policy and the policy can be mutually comprehensive.
  - At the *identity* level, a user can be identified from one domain in another domain.

Grid Security Challenges

- Integration with existing systems and techno logies
  - It is unrealistic to use a single security technology to address Grid security issues.
  - Existing security infrastructures cannot be replaced.
  - Thus, a Grid security architecture must be
    - Implemental,
    - Extensible, and
    - Integrate

Grid Security Requirements

- Authentication
  - Entities are provided with plug points for multiple authentication mechanisms.
- Delegation
  - Users can delegate their access rights to services.
  - Delegation policies also can be specified.
- Single Logon
  - An entity is allowed to have continuous access rights for some reasonable period with single authentication.

Grid Security Requirements

- Credential Lifespan and Renewal
  - A job initiated by a user may take longer than the life time of the user's initial credential.
  - In such case, the user needs to be notified prior to expiration of the credential, or be able to refresh it automatically.
- Authorization
  - Resources are used under a certain authorization policies.
  - A service provider can specify its own authorization policy, with which users can invoke those policies.

Grid Security Requirements

- Confidentiality
  - The confidentiality of the communication mechanism and messages or documents is supported.
- Message Integrity
  - It is ensured that unauthorized changes of messages or documents may be detected.
- Privacy
  - A service requester and a service provider enforce privacy policies.
- Other requirements
  - Policy exchange, secure logging, manageability, ...

Contents

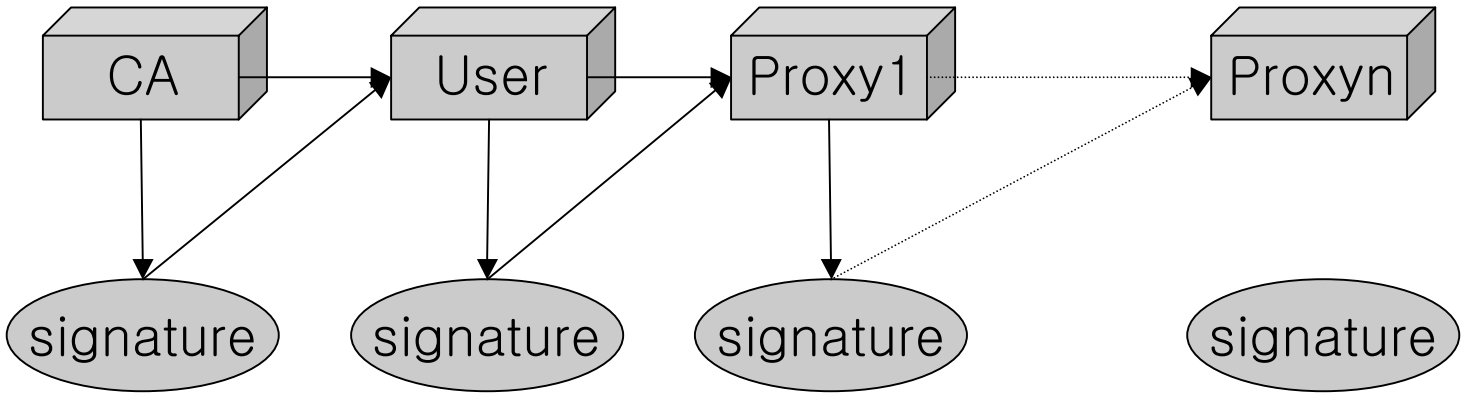
- Grid Security
  - Grid Security Challenges
  - Grid Security Requirements
- **Current Status of Grid Security**
  - Authentication and Delegation
  - Authorization
  - Grid Security Infrastructure (GSI)
  - OGSA
  - Web Services Security
- Things need more study
  - Authentication Interoperability
  - Fine-grained Authorization
- Summary

Authentication and Delegation (1/3)

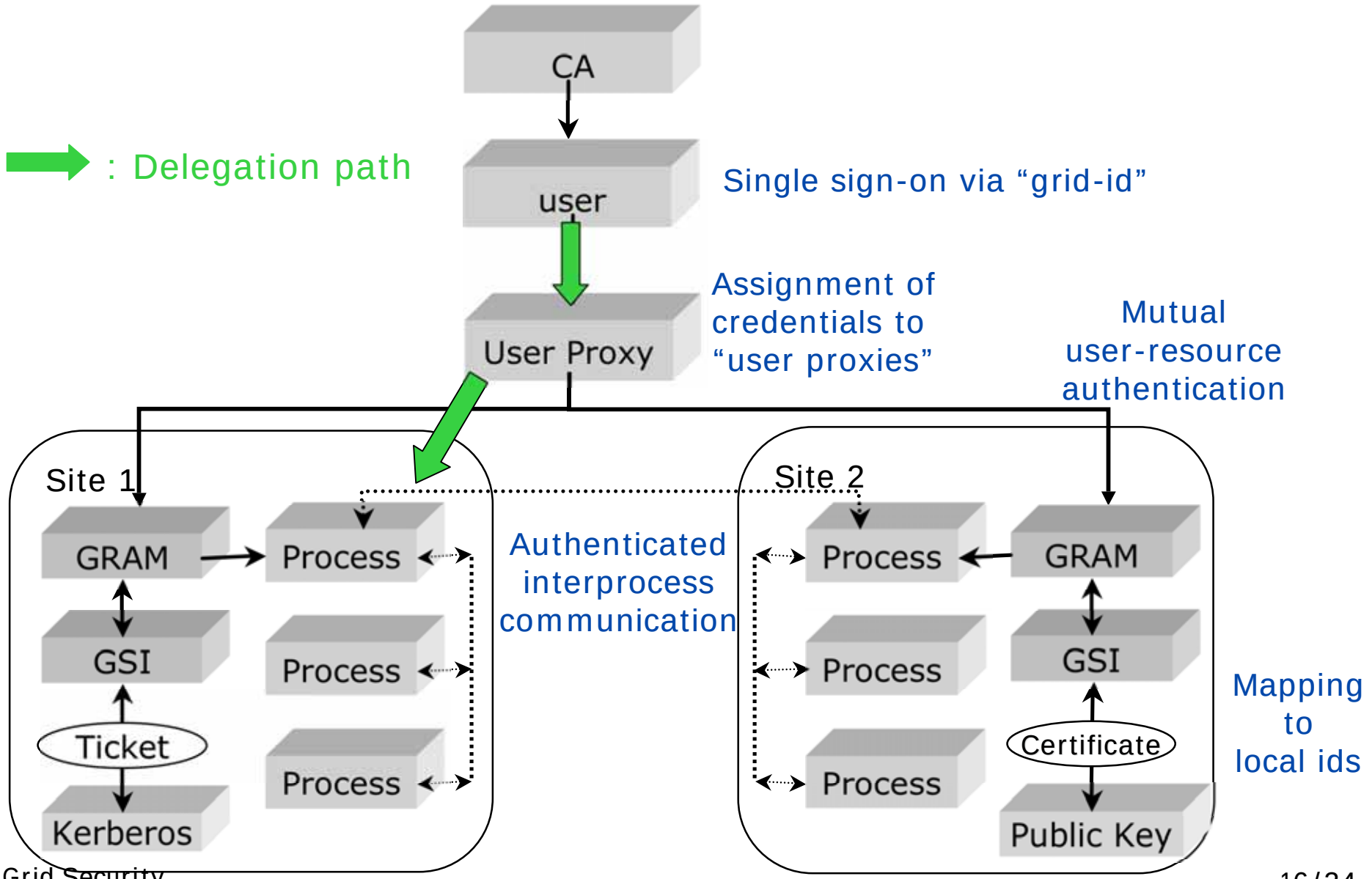
- The use of X.509 Certificates
  - Authentication by a distinguished name in a certificate under shared common CAs
  - Delegation and single sign-on through the use of X.509 proxy certificates
- Username and Password Authentication supported in GT4
  - Supporting WS-Security standard as opposed to X.509 credentials
  - Only providing authentication and not advanced features such as delegation, confidentiality, integrity, etc

Authentication and Delegation (2/3)

- Delegation of proxy certificates
  - Remote generation of user proxy
  - Generation of a new private key & certificate using the original key
  - Password or private key are not sent on network.



Authentication and Delegation (3/3)



Authorization (1/4)

- Users want to delegate their rights to proxies in other systems.
- Resource providers need an authorization service for user proxies submitted to their systems.
- Delegation is the process of transferring rights of users to tasks or proxies.
  - When too much rights are delegated, the abuse of rights is possible.
  - When too less rights are delegated, proxies cannot be executed completely.
- Thus, we need an authorization service in which users delegate restricted rights to proxies and resource providers can check valid uses of delegated rights.

Authorization (2/4)

- Pull Model
  - Granting a user's rights only on the specific conditions
  - Delegating rights which a user specifies
  - Managing rights with a user and resource providers
  - Example : Akenti

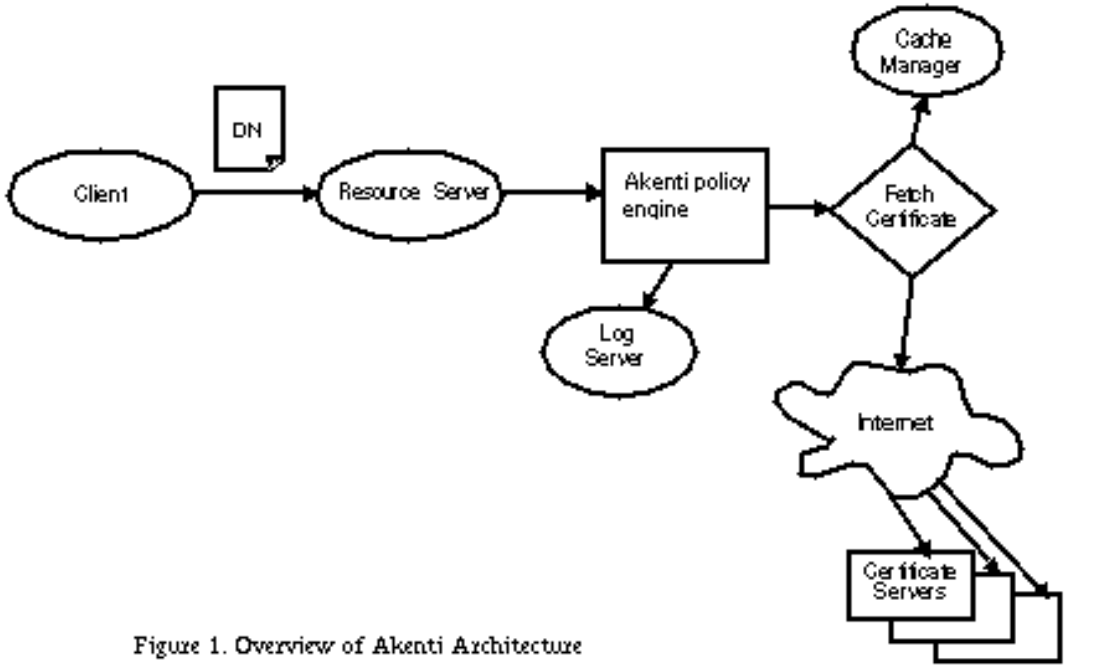
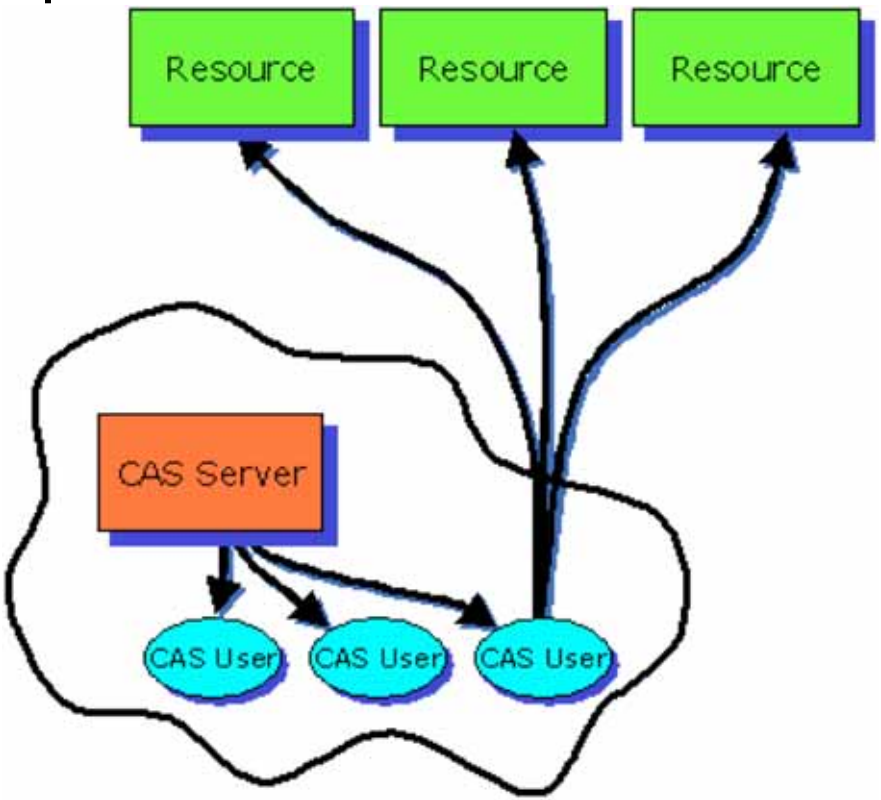


Figure 1. Overview of Akenti Architecture

Authorization (3/4)

- Push Model
  - Granting a user's rights according to his or her role
  - Managing rights with a central administrator
  - Example : CAS, PERMIS, VOMS



Authorization (4/4)

- Problems in related works
  - Akenti
    - Writing specific conditions and rights manually
    - Managing rights by users and resource providers
  - CAS
    - Delegating all rights owned by user's role
    - Not delegating restricted rights

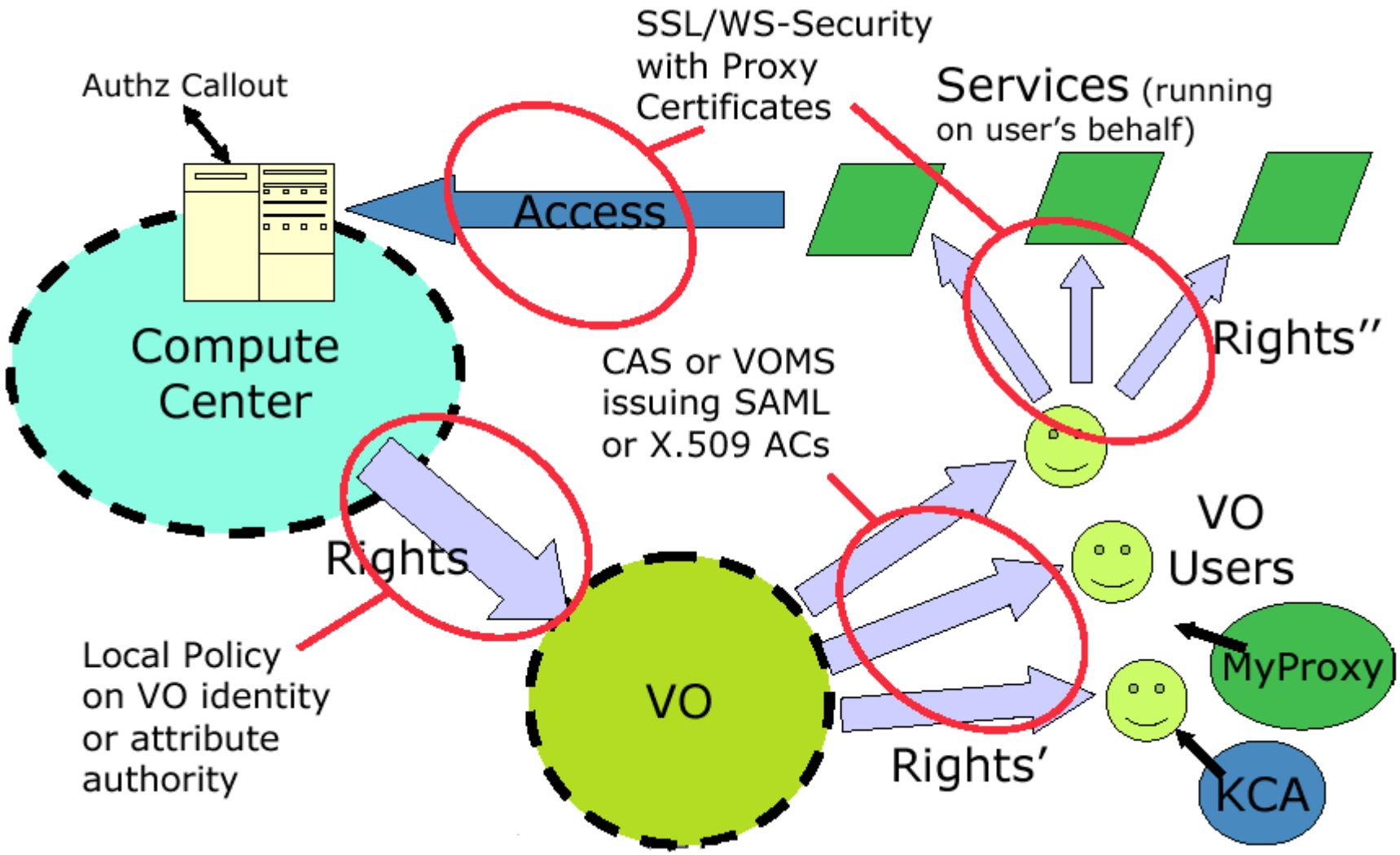
Grid Security Infrastructure (GSI)

- The fundamental security services in the Globus Toolkit
- Based on standard PKI technologies
  - SSL protocol for authentication, message protection
  - One-way, light-weight trust relationships by CAs
- X.509 Certificates for asserting identity
  - For users, services, hosts, etc
- Grid identity
  - A user is mapped to local identities using the distinguished name of the user's certificate.

Grid Security Infrastructure (GSI)

- X.509 Proxy Certificates
  - Enables single sign-on.
  - Allows users to delegate their identities and rights to services.
- Community Authorization Service (CAS)
  - Enables fine-grained authorization policy.
  - Resource providers set course-grained policy rules for foreign domain on CAS-identity.
  - CAS sets policy rules for its local users.
  - Requestors obtain capabilities from their local CAS.

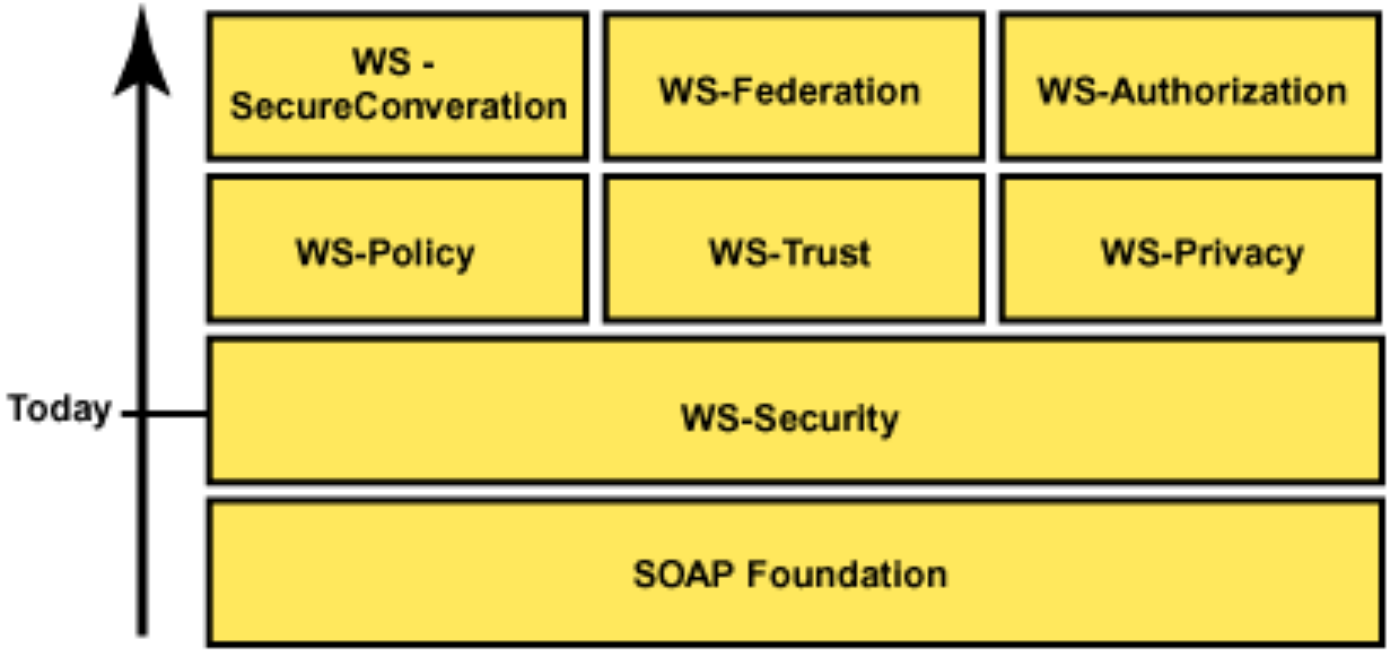
Grid Security Infrastructure (GSI)



Open Grid Services Architecture (OGSA)

- A Grid system architecture
  - Based on Web services and technologies
  - An open source collection of Grid services that follow OGSA principles are offered by the Globus project since GT3.0.
- WS-Resource Framework (WSRF)
  - A set of Web service specifications being developed by the OASIS organization
  - Describing how to implement OGSA capabilities using Web services
- Standardization
  - Underway in the Global Grid Forum (GGF) and OASIS
  - Many working groups on Grid security, such as OGSA Security, GSI, Authorization Frameworks and Mechanisms (AuthZ), Certificate Authority Operations (CAOPS), Grid Certificate Policy (GCP), and OGSA Authorization (OGSA-Authz)

Security in a Web Services World



- The Web services security roadmap provides a layered approach to address Web services.
- The OGSA security models needs to be consistent with Web services security model.

Contents

- Grid Security
  - Grid Security Challenges
  - Grid Security Requirements
- Current Status of Grid Security
  - Authentication and Delegation
  - Authorization
  - Grid Security Infrastructure (GSI)
  - OGSA
  - Web Services Security
- **Things need more study**
  - Authentication Interoperability
  - Fine-grained Authorization
- Summary

Authentication Interoperability

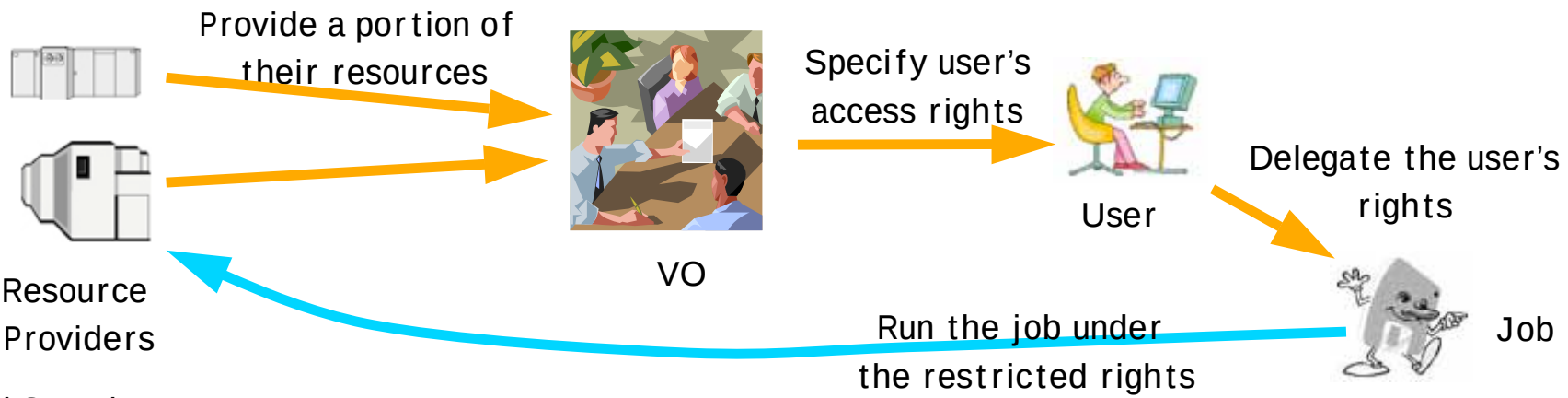
- Motivations
  - Use of different authentication schemes by different resource providers
  - Use of different policies for different resource providers and organizations
- Requirements
  - Need an interoperable authentication method
  - Need an automatic policy match and negotiation

Example Case

- Case
  - User A is given access rights to resources B and C when running a process D for some time.
  - How do we know he is accessing resources B and C for the process D?
  - How do we know he is not redoing the previously allowed job?
  - How do we know he has not exceeded his access time on using resources B and C in case that the resources given to the VO at which the user A belongs are larger than those given to the user A.
  - Etc…
- Need a fine control of resources
  - Also need for accounting

Fine-grained Authorization Service

- Motivations
  - Resource providers want their resources to be used by only VO members under their local polices.
  - VO managers specify user access rights.
  - A user delegates his or her rights to the job to run.
- Requirements
  - Combining polices from different sources
  - Fine-grained resource control
  - VO-based management of jobs and resources

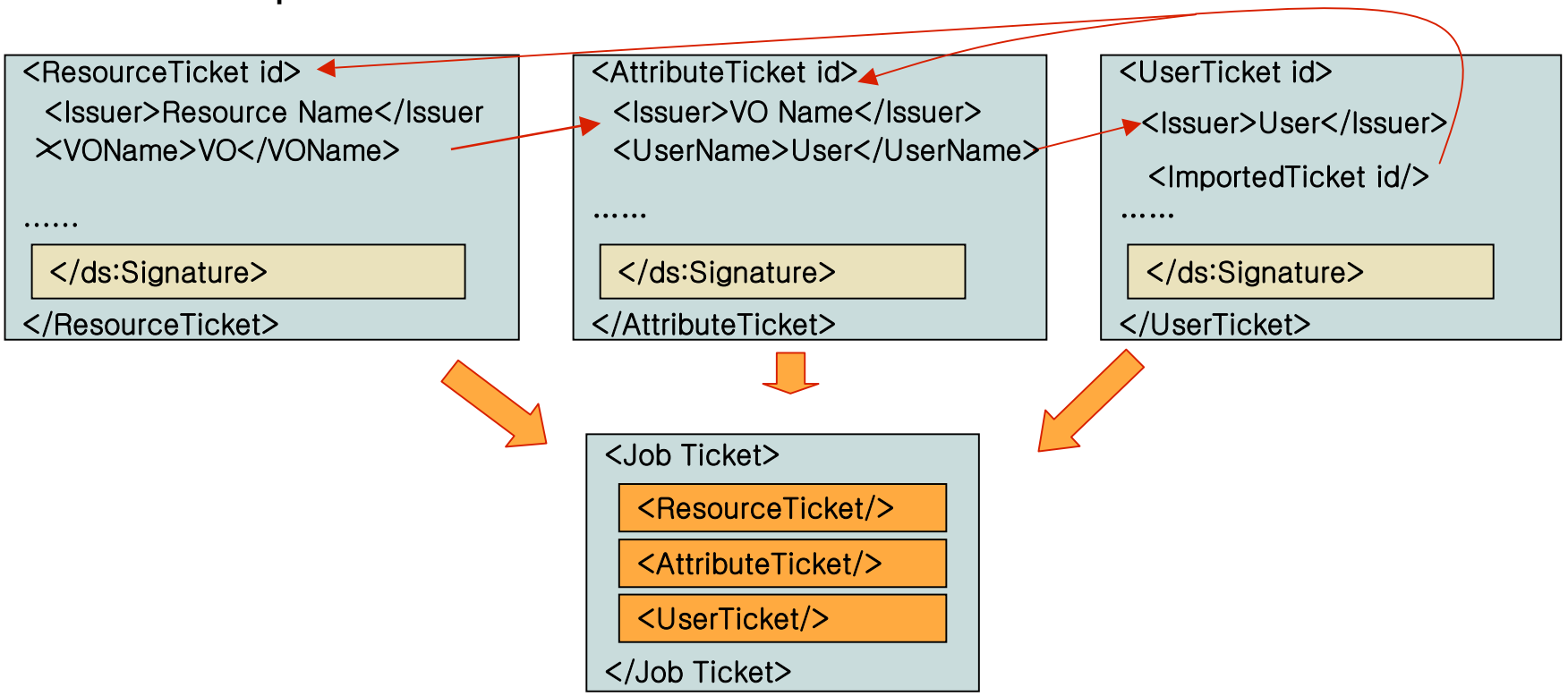


TAS : Tickets

- A ticket is an XML record asserting that the issuer specifies a policy.
  - A resource provider notifies the resource usage policy.
  - A VO manager issues VO users' attributes.
  - A user delegates his or her rights to the submitted job.
- Each ticket is signed by the private key of the issuer to protect the integrity of the ticket.
- Tickets are unforgeable and exchangeable among VO entities for resource control.
- Tickets are classified into
  - resource ticket,
  - attribute ticket,
  - user ticket, and
  - job ticket.

TAS : Job Ticket

- Generated by a user in order to request the rights
- Including necessary tickets for a job
  - Imported ticket field in the user ticket indicates other tickets.



TAS : Supported Grid Services

- Dynamic VO Management
  - A VO is easily managed by sharing resource and attribute tickets.
  - VO policies can be changed by re-issuing the corresponding tickets.
- Fine-grained Rights Delegation
  - Resource providers and VO managers delegate a set of permitted rights to users.
  - A user also delegates his or her rights to the job using the user ticket.

Summary

- Grid Security
  - Needs to solve many security issues to provide dynamic, scalable VOs in Grid computing environment.
  - Hard problem due to diversity, interoperability, integration, …
- Fine-grained Authorization Services
  - As a Grid security service, it needs VO-wide fine-grained authorization of jobs and resources.

References

- F. Siebenlist, V. Welch, “Grid Security : The Globus Perspective,” GlobusWORLD 2004, http://www.globus.org/
- V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke, “Security for Grid Services,” HPDC-12, June 2003.
- N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist, V. Welch, I. Foster, S. Tuecke, “The Security Architecture for Open Grid Services,” OGSA-SEC-WG document, GGF.
- S. H. Kim, J. Kim, S. J. Hong, S. W. Kim, "Workflow based Authorization Service in Grid", 4th International workshop on Grid Computing (Grid 2003), pp 94-100, Novebmer 2003.
- S. H. Kim, K. H. Kim, J. Kim, S. J. Hong, S. W. Kim, “Workflow-based Authorization Service in the Grid”, Journal of Grid Computing, vol. 2, no. 1, pp. 43-55, 2004.
- B. J. Kim, S. J. Hong, J. Kim, "Ticket-Based Fine-Grained Authorization Service in the Dynamic VO Environment," ACM Workshop on Secure Web Services, October 2004.
- B. J. Kim, K. H. Kim, S. J. Hong, J. Kim, "Ticket-based Grid Services Architecture for Dynamic Virtual Organizations,“ LNCS 3470 (Advances in Grid Computing: EGC 2005), pp. 394-403, 2005.