

A*STAR Grid Computing TSRP
<Middleware & Management>



Grid security: issues, challenges and approaches

Li Tieyan

InfoComm Security Department (ICSD)

Institute for Infocomm Research (I2R)

22nd, Sept. 2003

Outline

- Grid security issues
- Grid security challenges
- Initial proposals
 - Fingerprint authentication with smart card
 - Efficient certificate management
 - Sandboxing of applications
 - Others...

Objective: Finding niche areas to complement the grid security infrastructure, management and middleware.

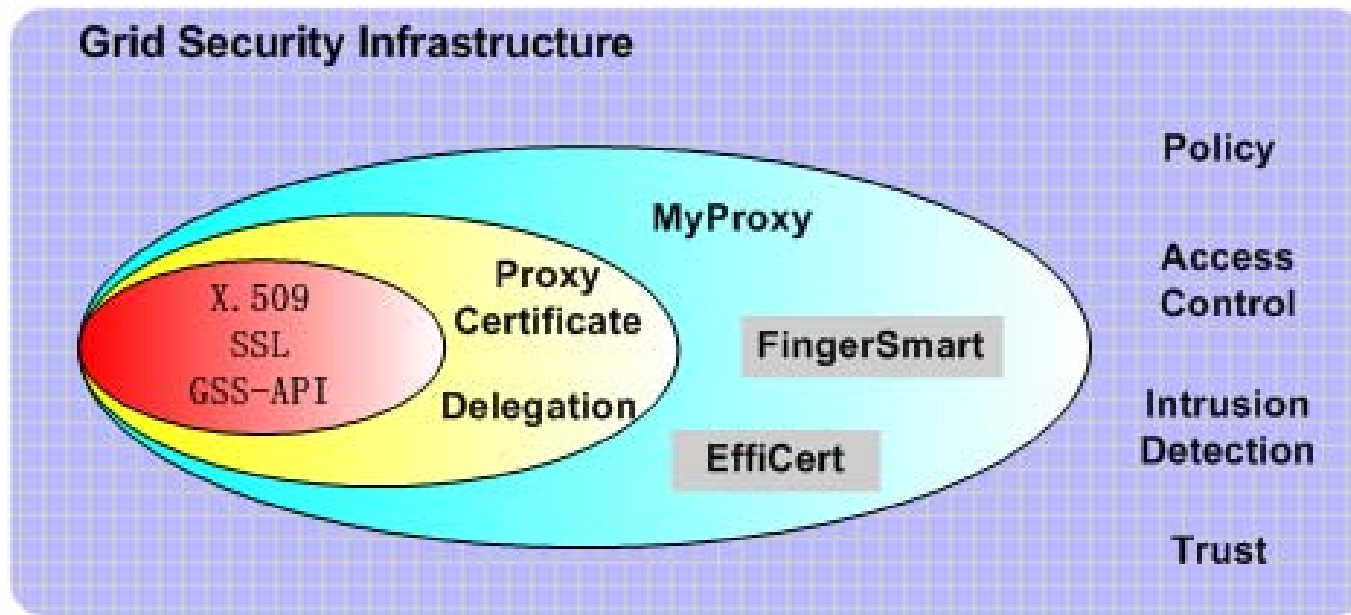
Grid security issues

- Generic security issues:
 - Authentication (X.509, proxy credentials)
 - Authorization (SAML)
 - Access control (XACML)
 - Accounting (Draft on requirement)
 - Application security
- On-going efforts on specifying open grid service architecture such as AAAA, specifically:
 - Grid users need to have strong protection mechanisms to securely store private keys.
 - There is no efficient revocation scheme for grid user certificates.
 - There is no efficient management scheme for VO management.
 - Grid applications are not executed securely.

Grid security challenges

We have also identified the following key challenges.

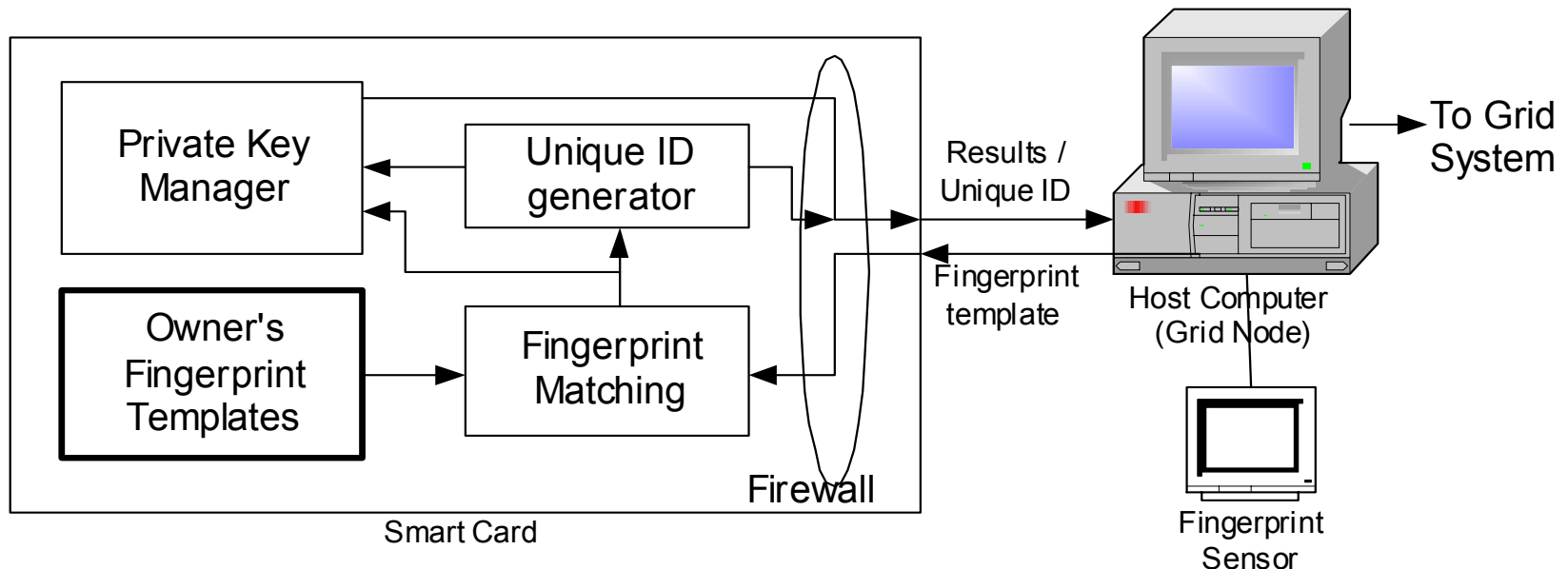
- How to protect the grid user key? (FingerSmart)
- How to efficiently manage the certificates? (Efficert)
- How to execute applications securely? (Sandboxing)
- How to manage the security of VO? (VO security management)



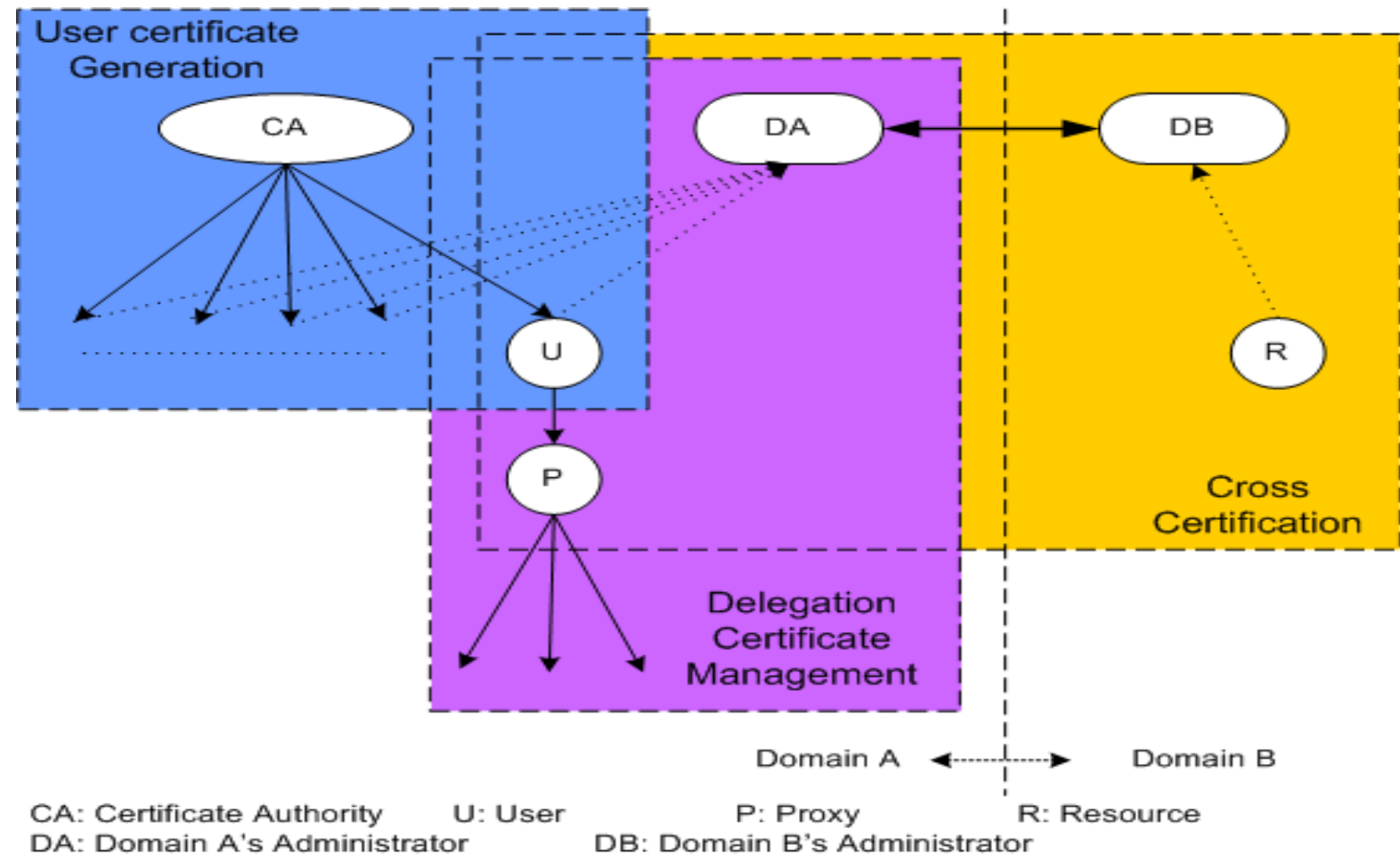
FingerSmart

Fingerprint Matching On Smart Card.

- Completed fingerprint matching on smart card, requiring only 500b RAM & 6Kb footprint.
- Targeted for Java Card, but can be customized for other smart card OS.



Efficient certificate management



Features

- Fingerprint Identification
- Biometric Registration/Verification for Multi-site
- Smart card private key protection
- CA based User key generation
- User based delegation key generation
- Efficient certificate revocation
- Semi-trusted online domain administrator
- Cross certification

Sandboxing of Applications

- In grid computing model, compute resources are commoditized.
- User who has need for off-site compute resources response to advertisement
- User submit job.

Application Sandbox Scenario I

- User submit job in the application domain
- Job has trojan or rogue program with ulterior intents to
 - Acquire resource availability outside its application domain
 - Peek into activities or data of other client-users-commercial espionage.
- Solution approach
 - Verification, certification of application
 - Monitoring of domain activities

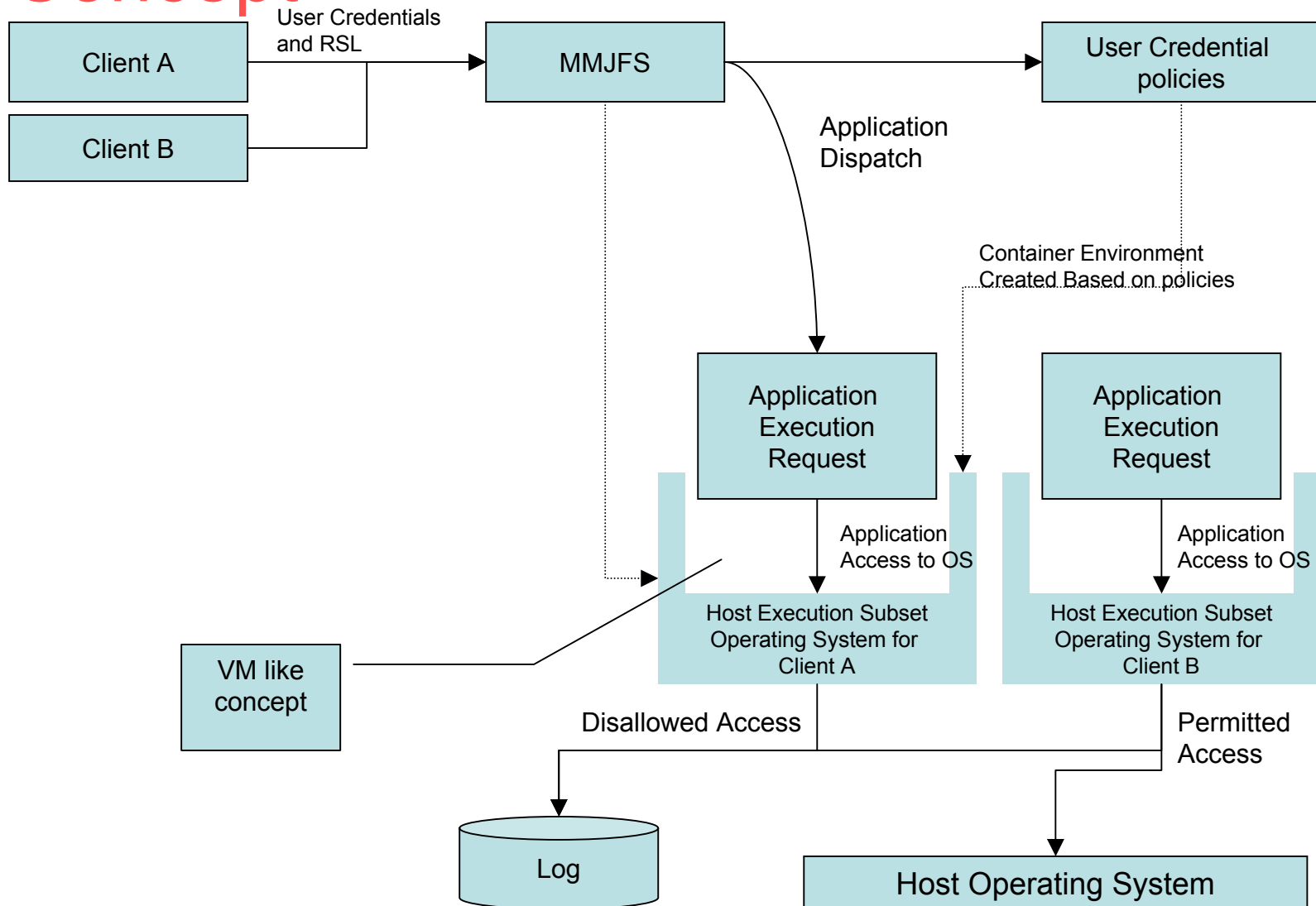
Application sandbox Scenario II

- User submit job in the application domain
- Unauthorised access of domain by external party – commercial espionage
- Solution approach:
 - Fencing of domain
- Research proposal (Dr. Daniel Tan, NTU)
 - Together with Middleware Group, to develop an application domain control and monitoring system

Application Sand Box Execution Environment

- Hides complexity of host under standard interface
- Contains all execution of application within a user space process
- Provides extensive logging capabilities of executed process
- Protects host environment from unauthorized access of local file-system
- Prevents use of unauthorized applications and files on the host system
- Allows resource representation in a more controllable manner

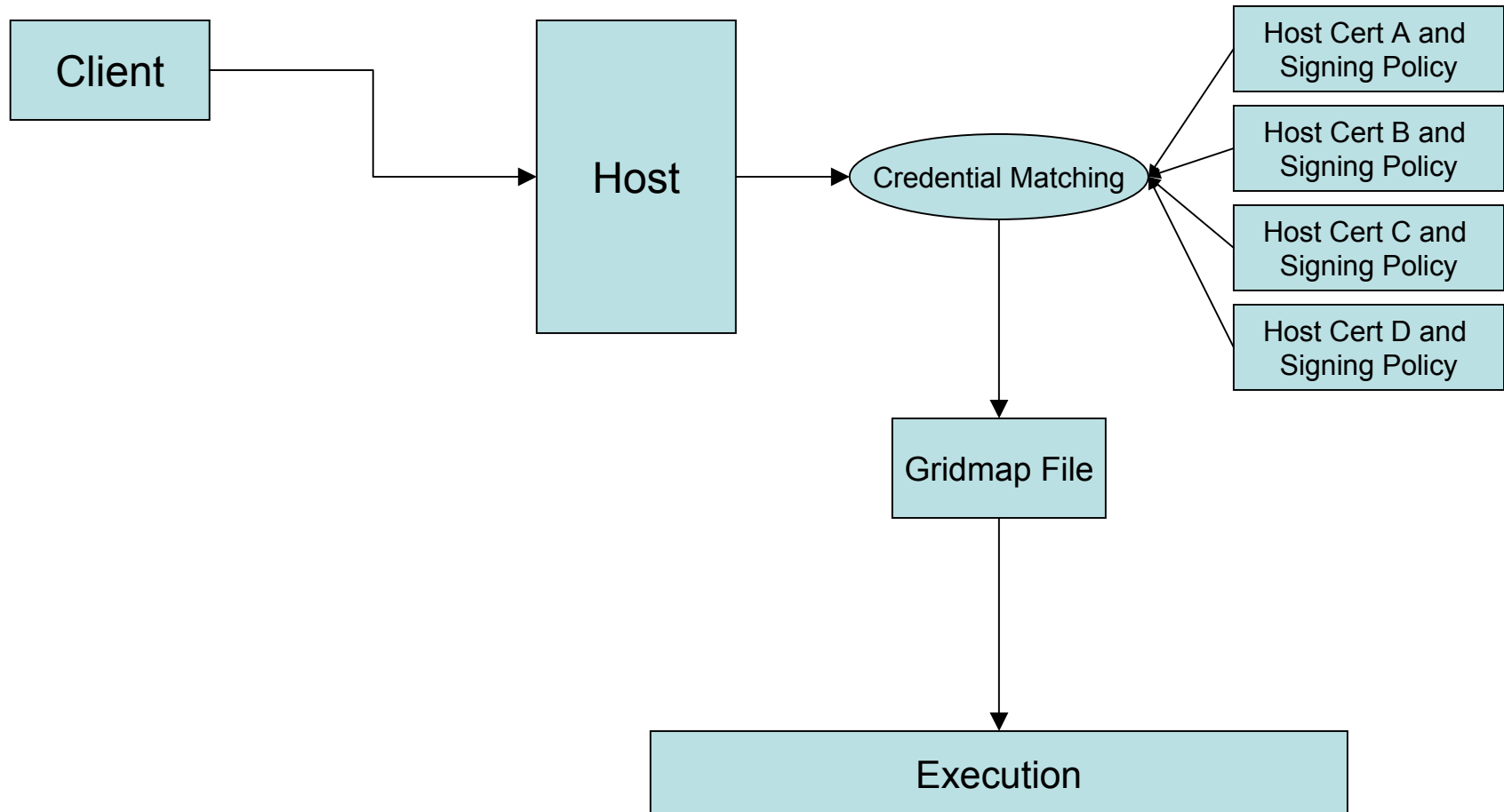
Application Sand Box Execution Concept



Multi Grid Trust

- Allow formation of a single resource pool from multiple Grids
- Joining of Grids based on local administrator choice

Multi Grid Trust



Virtual Organization

- **VO (Virtual Organization)**
 - Abstraction to model distributed resource sharing and allocation across different organizational entities
- **With the notion of VO, the Grid Computing System can:**
 - Support applications beyond scientific computing
 - Simplify the design and implementation of such applications
 - Implement distributed systems with more complex inter-process relationships
- Security mechanisms are needed for management of VO

Security of VO management

➤ **Management of VO**

- Discover VO by Grid participants
- Authentication and authorization of participants to join VO
- Access control: Participants access shared resources in VO
- Access control: Participants and their associated resources accessed by VO

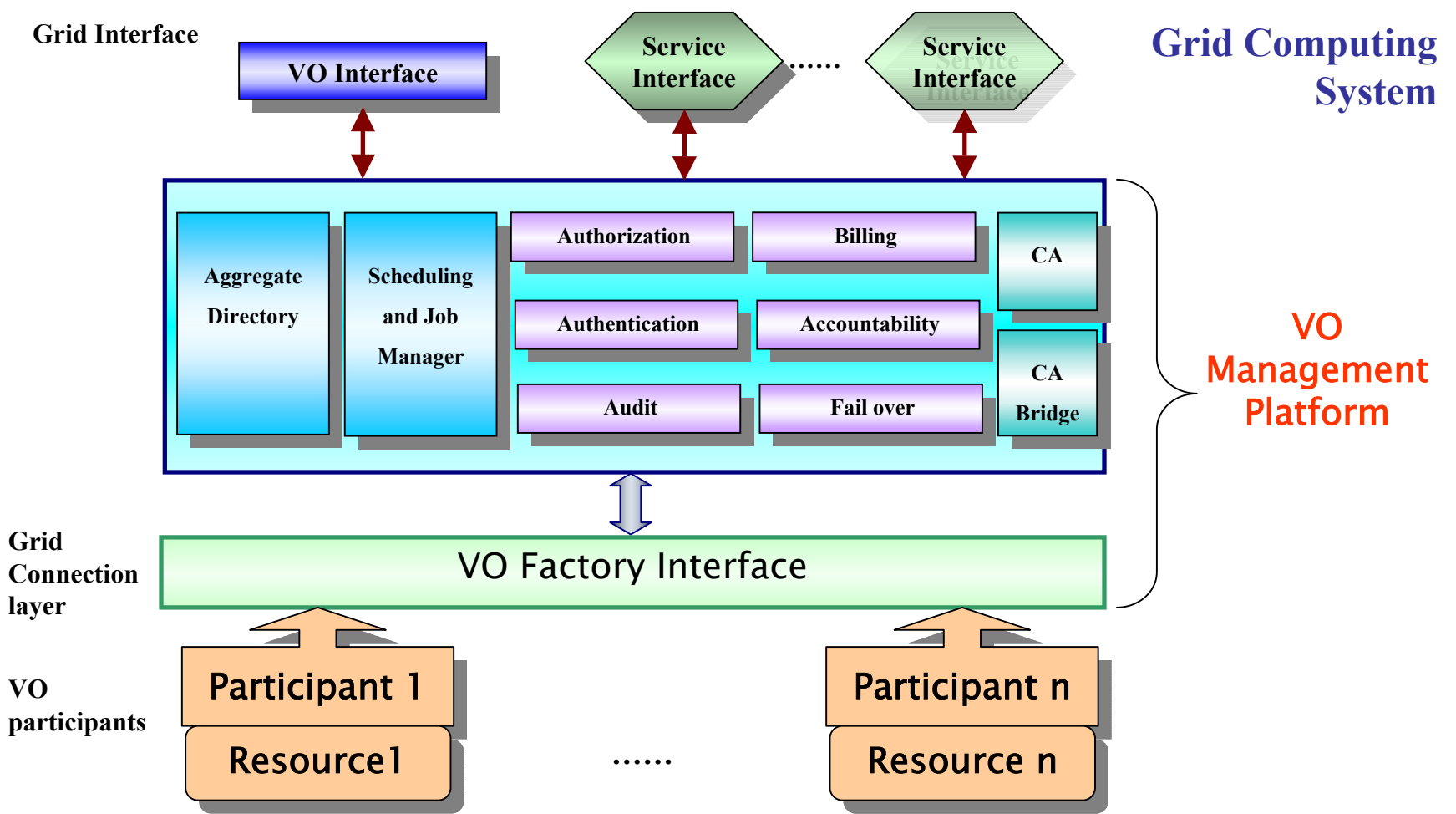
➤ **The challenges of VO security**

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

Directory service of VO management

- Directory Service facilitates operations of VO:
 - Access resources
 - Manage resources
 - Organize and store information about shared resources
- Design challenges of the Directory Service for VO management are:
 - Dynamic
 - Robust
 - Highly available
- Aims to build a highly available Directory Service suitable for VO management and Grid applications

VO management platform



To do list:

- Stage 1
 - EffiCert
 - FingerSmart
 - Sandboxing
 - VO security management
- Stage 2
 - Developing secure applications based on EffiCert, FingerSmart, Sandboxing and VO management
- Stage 3
 - Implementation and testing

Thank you!

Q & A