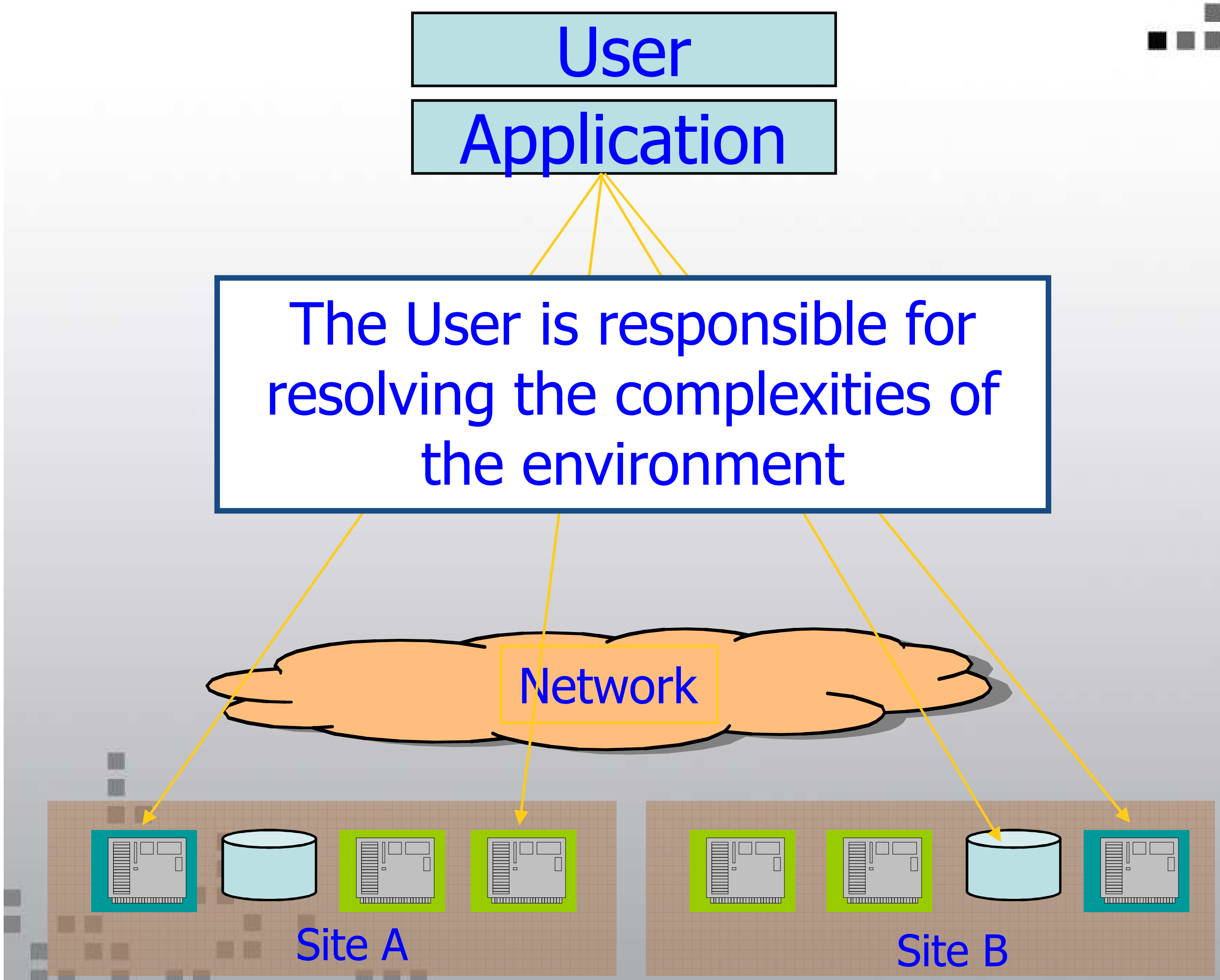
Globus Toolkit - 4

Overview

- Grid Architecture
- Globus Toolkit -4 Architecture
- Components in Globus Toolkit -4

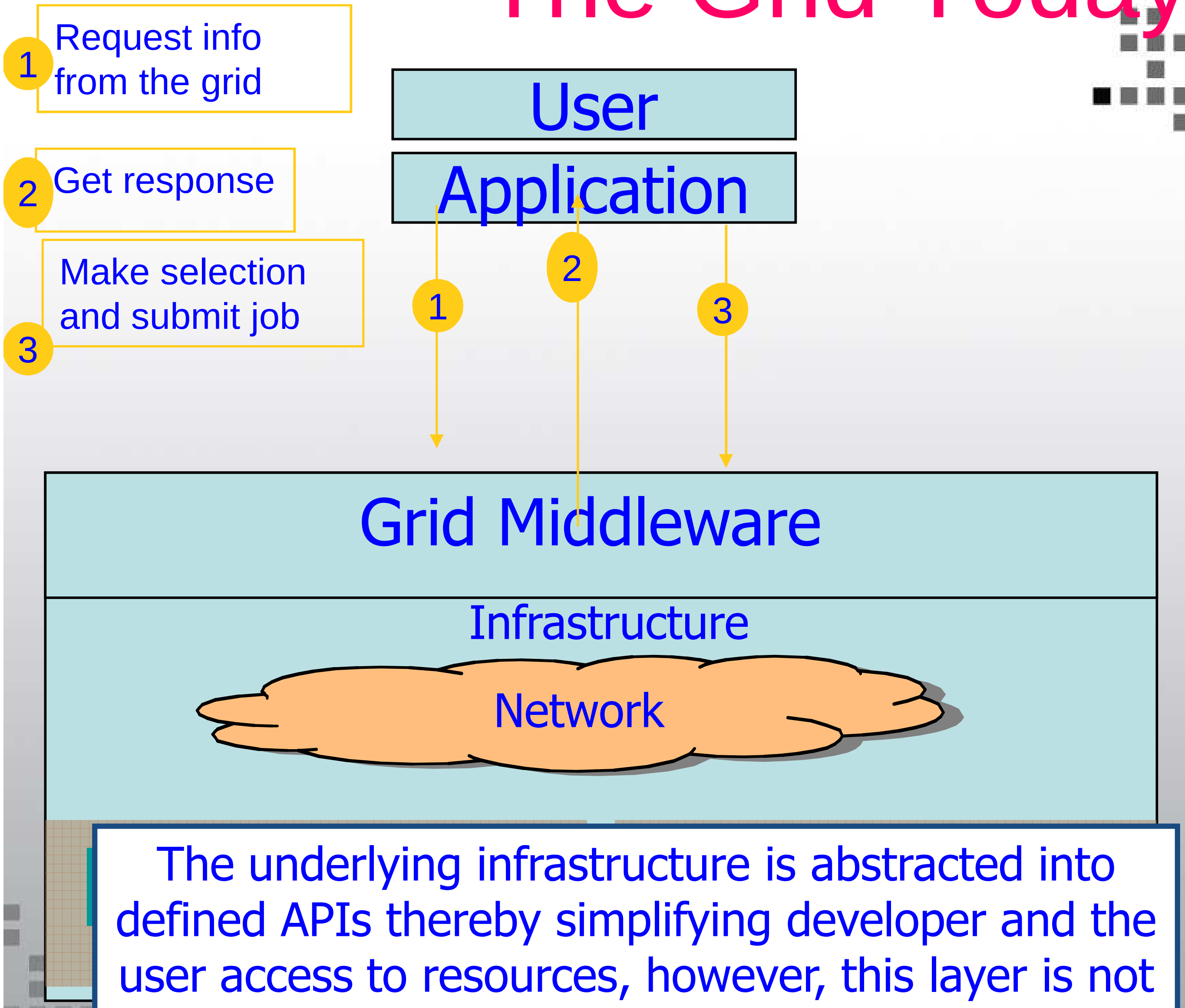
Before the Grid



User
Application
The User is responsible for resolving the complexities of the environment
Network
Site A
Site B

- independent sites
- independent hardware and software
- independent user ids
- security policy requiring local connection to the machine.

The Grid Today



The underlying infrastructure is abstracted into defined APIs thereby simplifying developer and the user access to resources, however, this layer is not intelligent

Common Middleware

- abstracts independent, hardware, software, user ids, into a service layer with defined APIs
- comprehensive security,
- allows for site autonomy
- provides a common infrastructure based on middleware

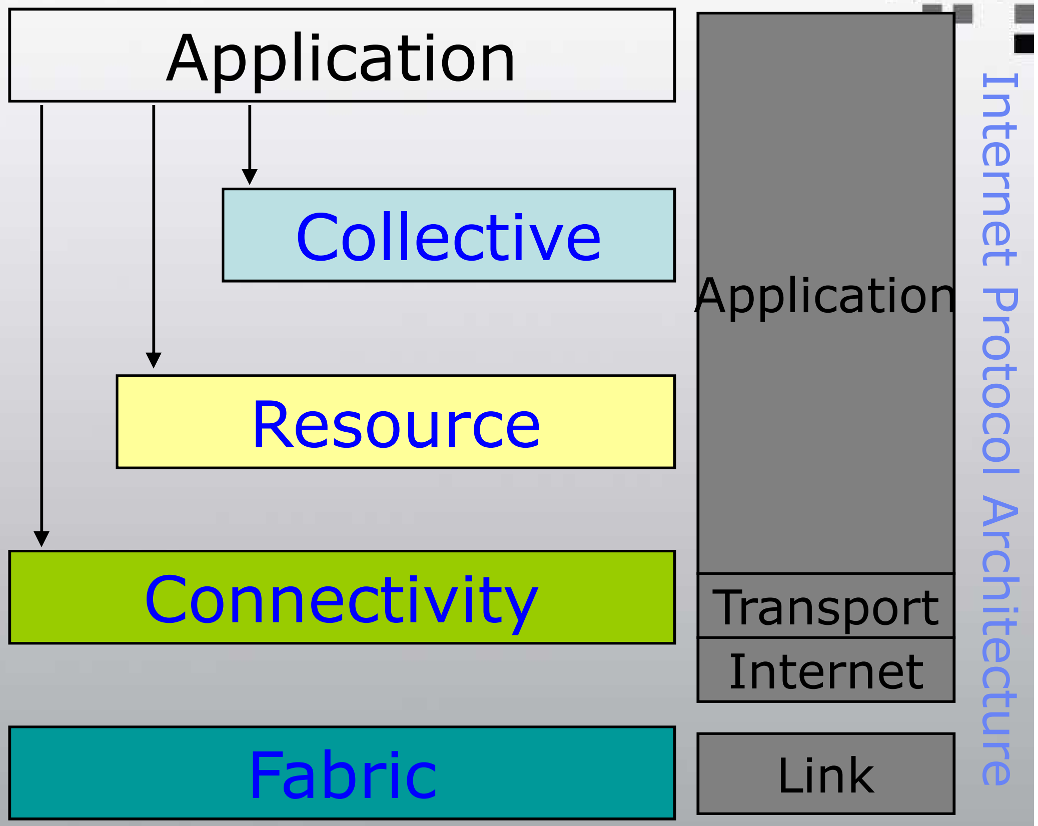
Layered Grid Architecture (By Analogy to Internet Architecture)

“Coordinating multiple resources”: ubiquitous infrastructure services, app-specific distributed services

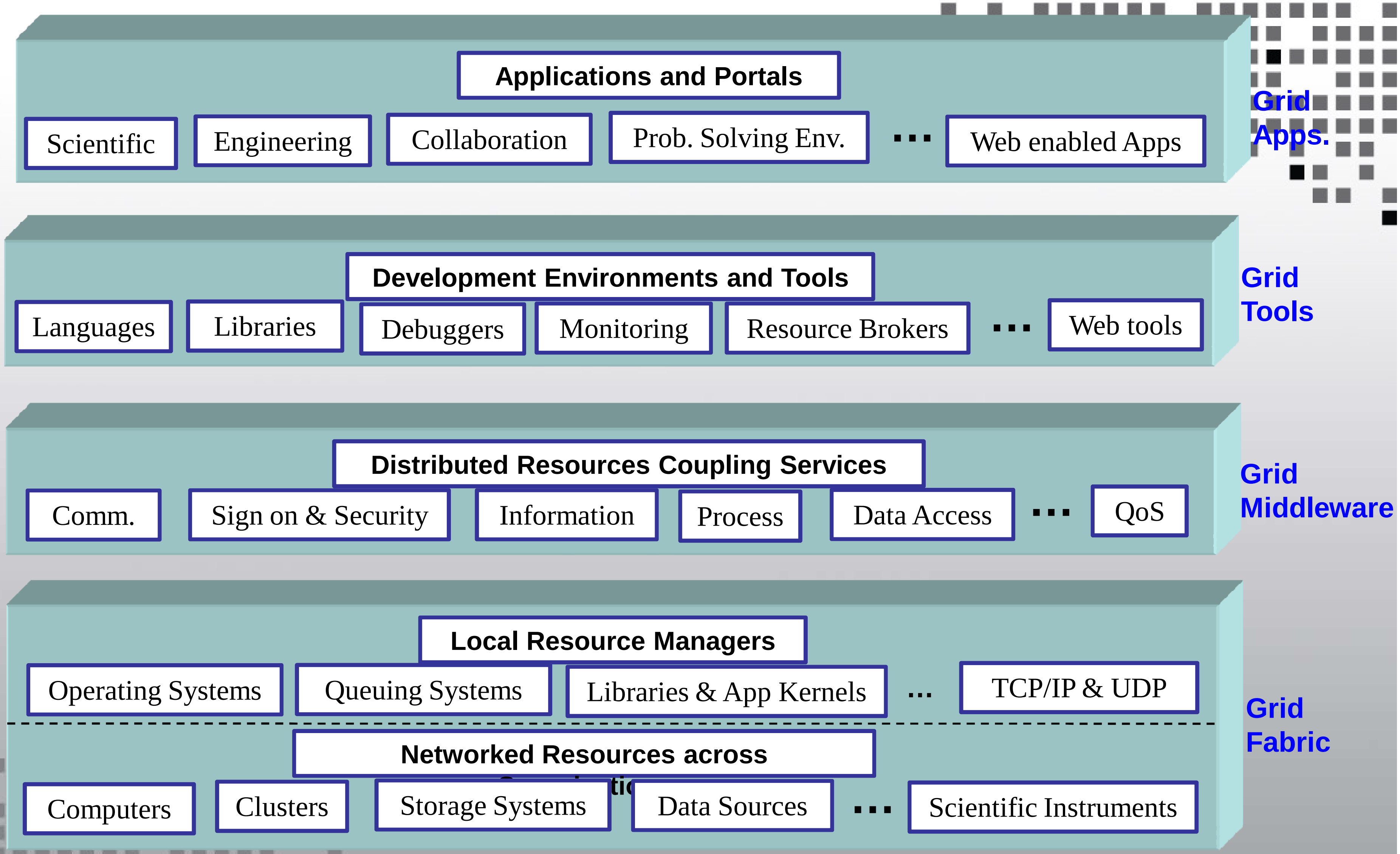
“Sharing single resources”: negotiating access, controlling use

“Talking to things”: communication (Internet protocols) & security

“Controlling things locally”: Access to, & control of, resources



Grid Components



Applications and Portals

Scientific | Engineering | Collaboration | Prob. Solving Env. | … | Web enabled Apps

Grid Apps.

Development Environments and Tools

Languages | Libraries | Debuggers | Monitoring | Resource Brokers | … | Web tools

Grid Tools

Distributed Resources Coupling Services

Comm. | Sign on & Security | Information | Process | Data Access | … | QoS

Grid Middleware

Local Resource Managers

Operating Systems | Queuing Systems | Libraries & App Kernels | … | TCP/IP & UDP

Networked Resources across

tic

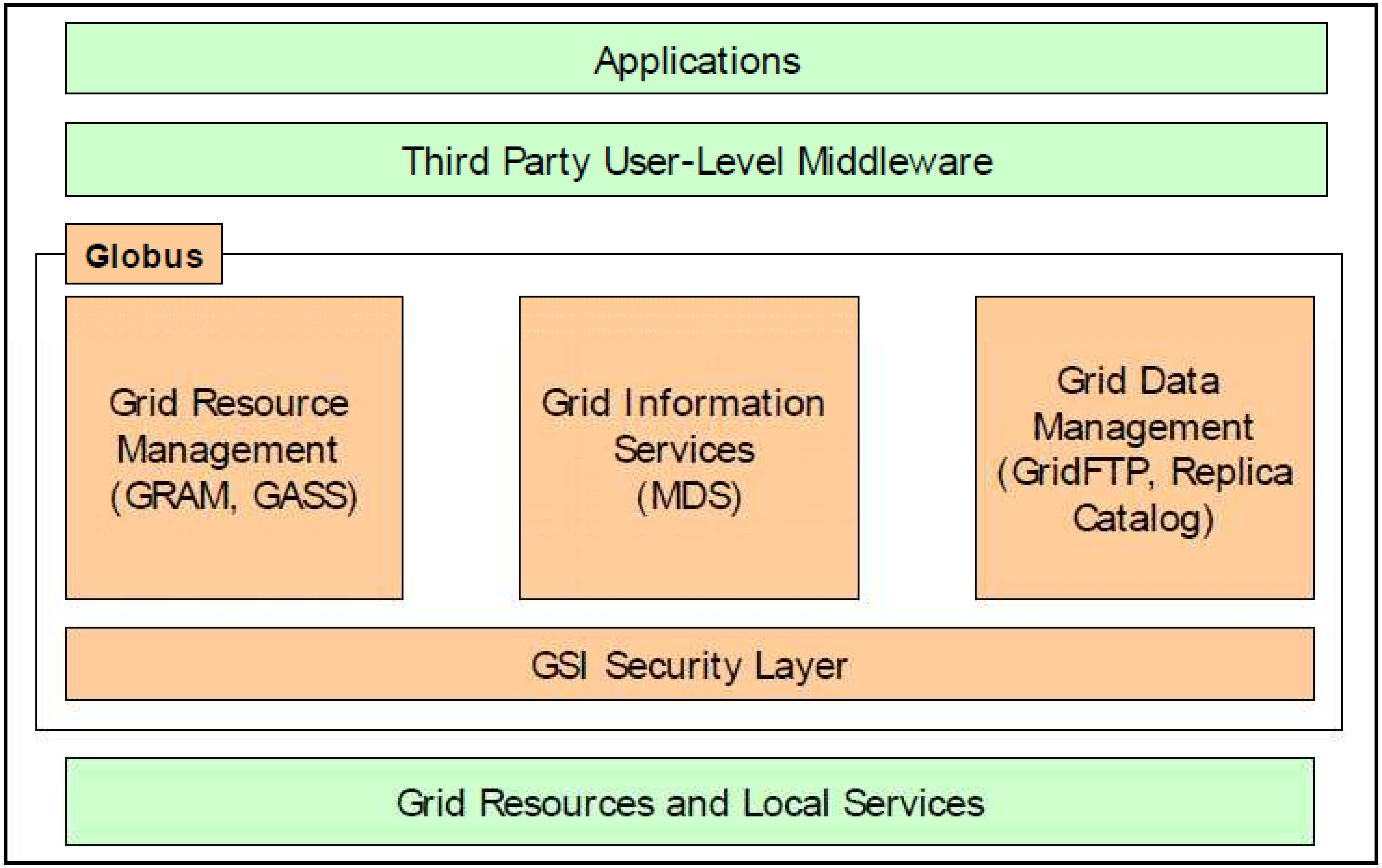
Computers | Clusters | Storage Systems | Data Sources | … | Scientific Instruments

Grid Fabric

Globus Toolkit

- The Globus project provides open source software toolkit that can be used to build computational grids and grid based applications.
- It allows sharing of computing power, databases, and other tools securely online across corporate, institutional and geographic boundaries without sacrificing local autonomy.

Globus Toolkit



Applications

Third Party User-Level Middleware

Globus

Grid Resource Management (GRAM, GASS)

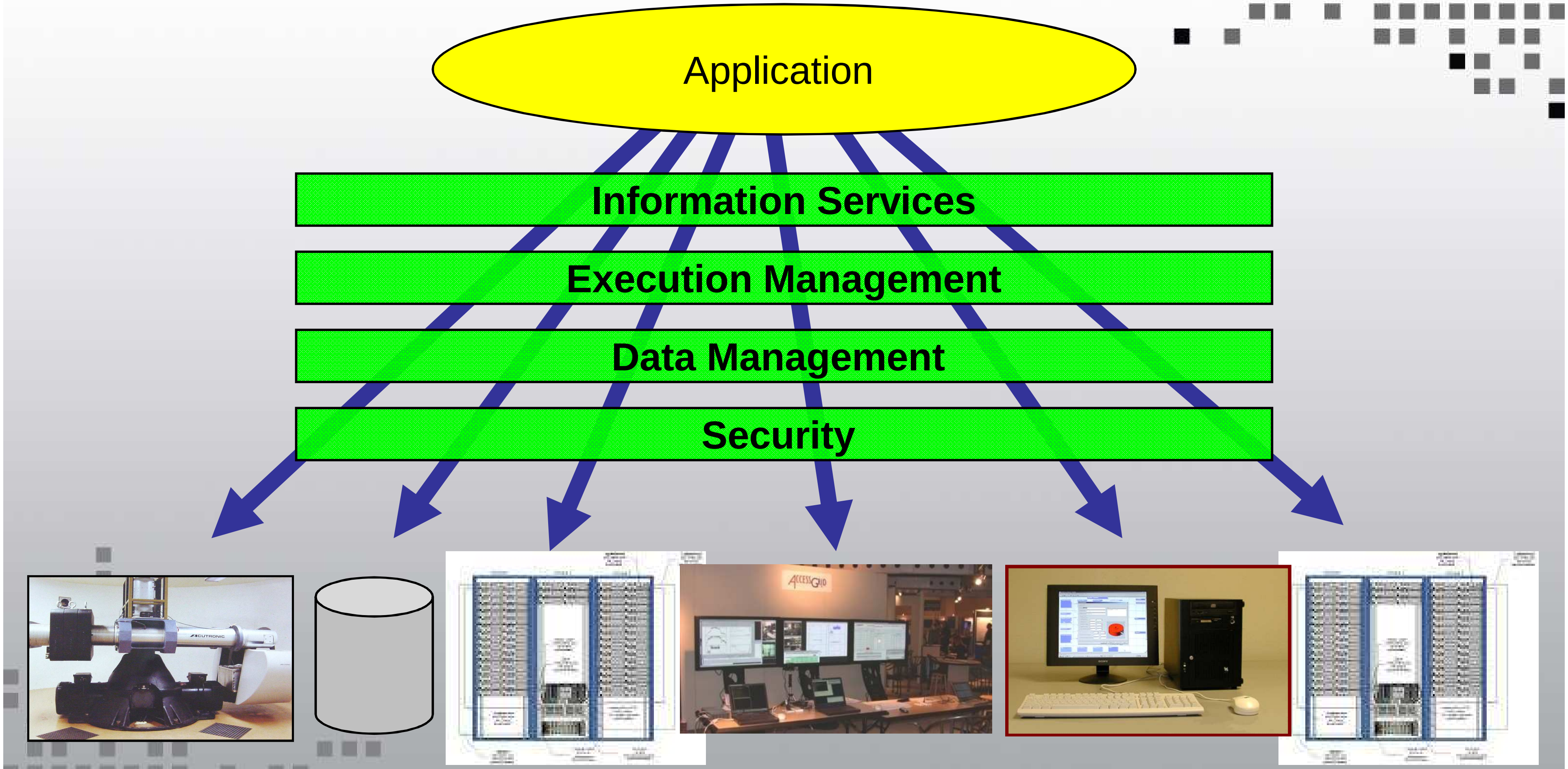
Grid Information Services (MDS)

Grid Data Management (GridFTP, Replica Catalog)

GSI Security Layer

Grid Resources and Local Services

Grid Infrastructure



Application

Information Services

Execution Management

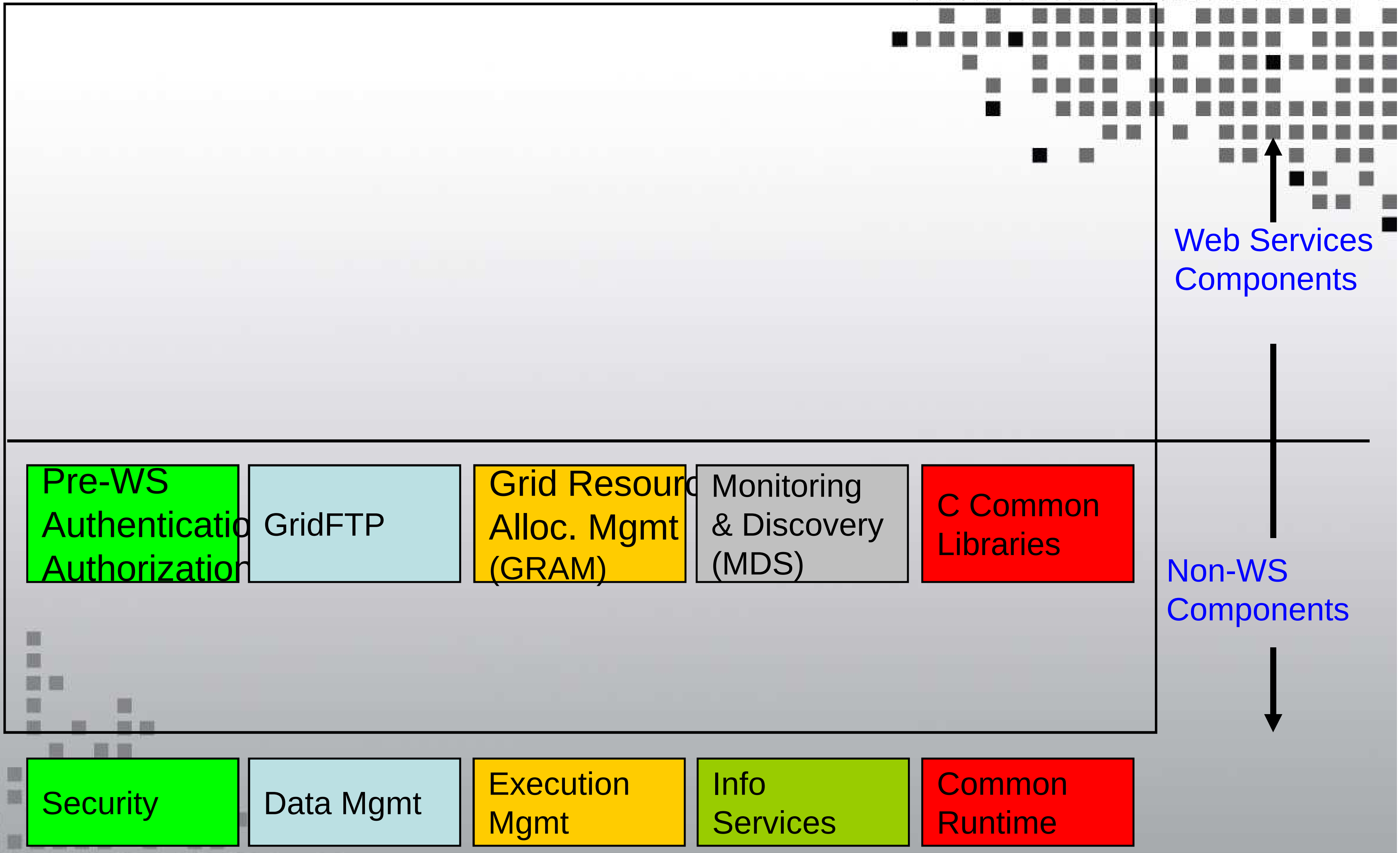
Data Management

Security

Globus Toolkit: Basic Grid Services

- Globus Toolkit Core
  - Infrastructure for building Grid services
  - Uniform, standard, WS-based protocols
  - Implementations in Java, C, Python, WSRF.NET
- Information Services
  - Discover & monitor dynamic services
- Execution Management
  - Provision environments, execute jobs, manage instruments
- Data management
  - Discover, transfer, & access large data
- Security
  - Authentication & Authorization
  - Credential management tools

From Globus Toolkit version 2 (GT2)



Web Services Components

Non-WS Components

Pre-WS Authenticatio Authorization

GridFTP

Grid Resourc Alloc. Mgmt (GRAM)

Monitoring & Discovery (MDS)

C Common Libraries

Security

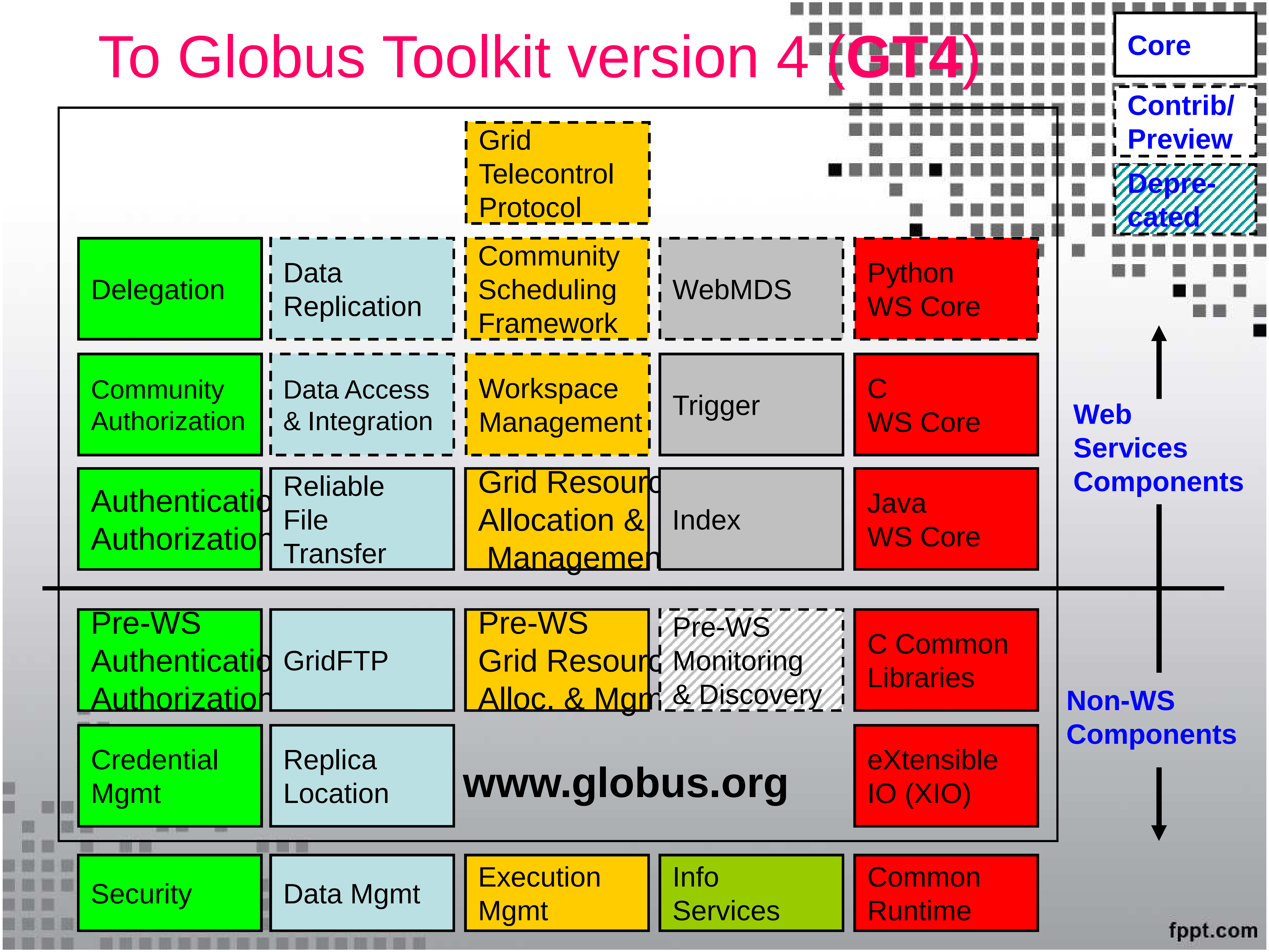
Data Mgmt

Execution Mgmt

Info Services

Common Runtime

To Globus Toolkit version 4 (GT4)



Core

Contrib/ Preview

Depre-cated

		Grid Telecontrol Protocol		
Delegation	Data Replication	Community Scheduling Framework	WebMDS	Python WS Core
Community Authorization	Data Access & Integration	Workspace Management	Trigger	C WS Core
Authenticatio Authorizatio	Reliable File Transfer	Grid Resourc Allocation & Managemen	Index	Java WS Core
Pre-WS Authenticatio Authorizatio	GridFTP	Pre-WS Grid Resourc Alloc. & Mgm	Pre-WS Monitoring & Discovery	C Common Libraries
Credential Mgmt	Replica Location	www.globus.org		eXtensible IO (XIO)
Security	Data Mgmt	Execution Mgmt	Info Services	Common Runtime

Web Services Components

Non-WS Components

fppt.com

Four Key Protocols

- The Globus Toolkit™ centers around four key protocols
  - Connectivity layer:
    - ***Security***: Grid Security Infrastructure (GSI)
  - Resource layer:
    - ***Resource Management***: Grid Resource Allocation Management (GRAM)
    - ***Information Services***: Grid Resource Information Protocol (GRIP)
    - ***Data Transfer***: Grid File Transfer Protocol (GridFTP)

The Globus Toolkit™: Security Services

The Globus Project™

Argonne National Laboratory
USC Information Sciences Institute

http://www.globus.org

GSI Security Layer

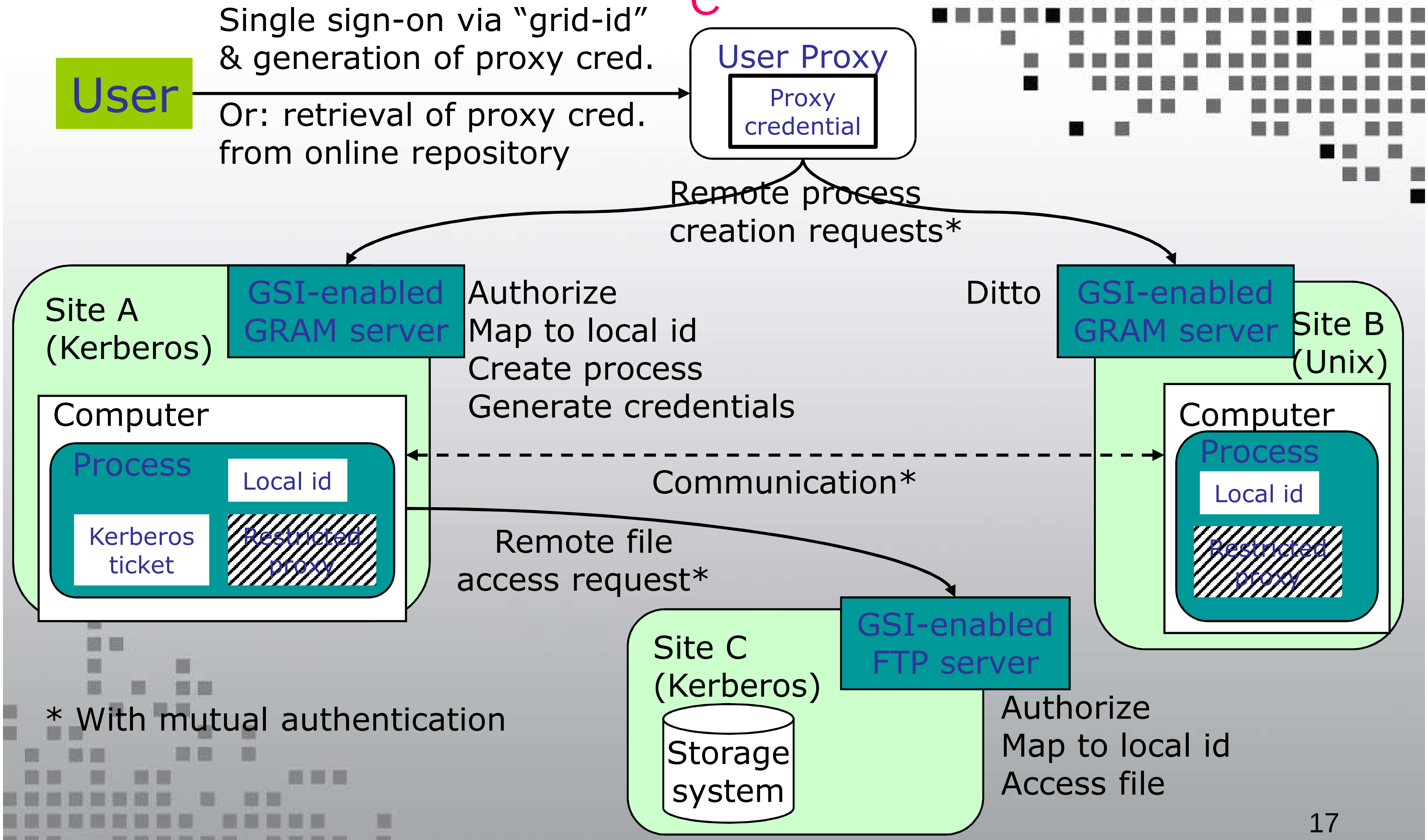
- The Grid Security Infrastructure (GSI) provides methods for authentication of Grid users and secure communication.
- It is based on SSL (Secure Sockets Layer), PKI (Public Key Infrastructure) and X.509 Certificate Architecture. The GSI provides services, protocols and libraries to achieve the following aims for Grid security:
  - Single sign-on for using Grid services through user certificates
  - Resource authentication through host certificates
  - Data encryption
  - Authorization
  - Delegation of authority and trust through proxies and certificate chain of trust for Certificate Authorities(CAs)
- Users gain access to resources by having their Grid certificate subjects mapped to an account on the remote machine by its system administrators.

Grid Security Infrastructure (GSI)

- Extensions to standard protocols & APIs
  - Standards: SSL/TLS, X.509 & CA, GSS-API
  - Extensions for single sign-on and delegation
- Globus Toolkit reference implementation of GSI
  - SSLeay/OpenSSL + GSS-API + SSO/delegation
  - Tools and services to interface to local security
    - Simple ACLs; SSLK5/PKINIT for access to K5, AFS; …
  - Tools for credential management
    - Login, logout, etc.
    - Smartcards
    - MyProxy: Web portal login and delegation
    - K5cert: Automatic X.509 certificate creation

GSI in Action

“Create Processes at A and B that Communicate & Access Files at C”



User

Single sign-on via “grid-id” & generation of proxy cred.

Or: retrieval of proxy cred. from online repository

User Proxy

Proxy credential

Remote process creation requests*

Site A (Kerberos)

GSI-enabled GRAM server

Authorize
Map to local id
Create process
Generate credentials

Computer

Process

Local id

Kerberos ticket

Restricted proxy

Ditto

GSI-enabled GRAM server

Site B (Unix)

Computer

Process

Local id

Restricted proxy

Communication*

Remote file access request*

Site C (Kerberos)

GSI-enabled FTP server

Storage system

Authorize
Map to local id
Access file

* With mutual authentication

Review of Public Key Cryptography

- Asymmetric keys
  - A **private** key is used to encrypt data.
  - A **public** key can decrypt data encrypted with the private key.
- An X.509 certificate includes…
  - Someone's subject name (user ID)
  - Their public key
  - A "signature" from a Certificate Authority (CA) that:
    - Proves that the certificate came from the CA.
    - Vouches for the subject name
    - Vouches for the binding of the public key to the subject

Public Key Based Authentication

- User encodes the data with private key
  - Possession of private key means you can authenticate as subject in certificate
- Public key is used to decode the data.
  - If you can decode it, you know the subject
- Treat your private key carefully!!
  - Private key is stored only in well-guarded places, and only in encrypted form

User Proxies

- Minimize exposure of user’s private key
- A temporary, X.509 proxy credential for use by our computations
  - We call this as user proxy certificate
  - Allows process to act on behalf of user
  - User-signed user proxy cert stored in local file
  - Created via “grid-proxy-init” command
- Proxy’s private key is not encrypted
  - Rely on file system security, proxy certificate file must be readable only by the owner

Delegation

- Remote creation of a user proxy
- Results in a new private key and X.509 proxy certificate, signed by the original key
- Allows remote process to act on behalf of the user
- Avoids sending passwords or private keys across the network

GSI Applications

- Globus Toolkit™ uses GSI for authentication
- Many Grid tools, directly or indirectly, e.g.
  - Condor-G, SRB, MPICH-G2, Cactus, GDMP, …
- Commercial and open source tools, e.g.
  - ssh, ftp, cvs, OpenLDAP, OpenAFS
  - SecureCRT (Win32 ssh client)
- And since we use standard X.509 certificates, they can also be used for
  - Web access, LDAP server access, etc.

The Globus Toolkit™: Resource Management Services

The Globus Project™

Argonne National Laboratory
USC Information Sciences Institute

http://www.globus.org

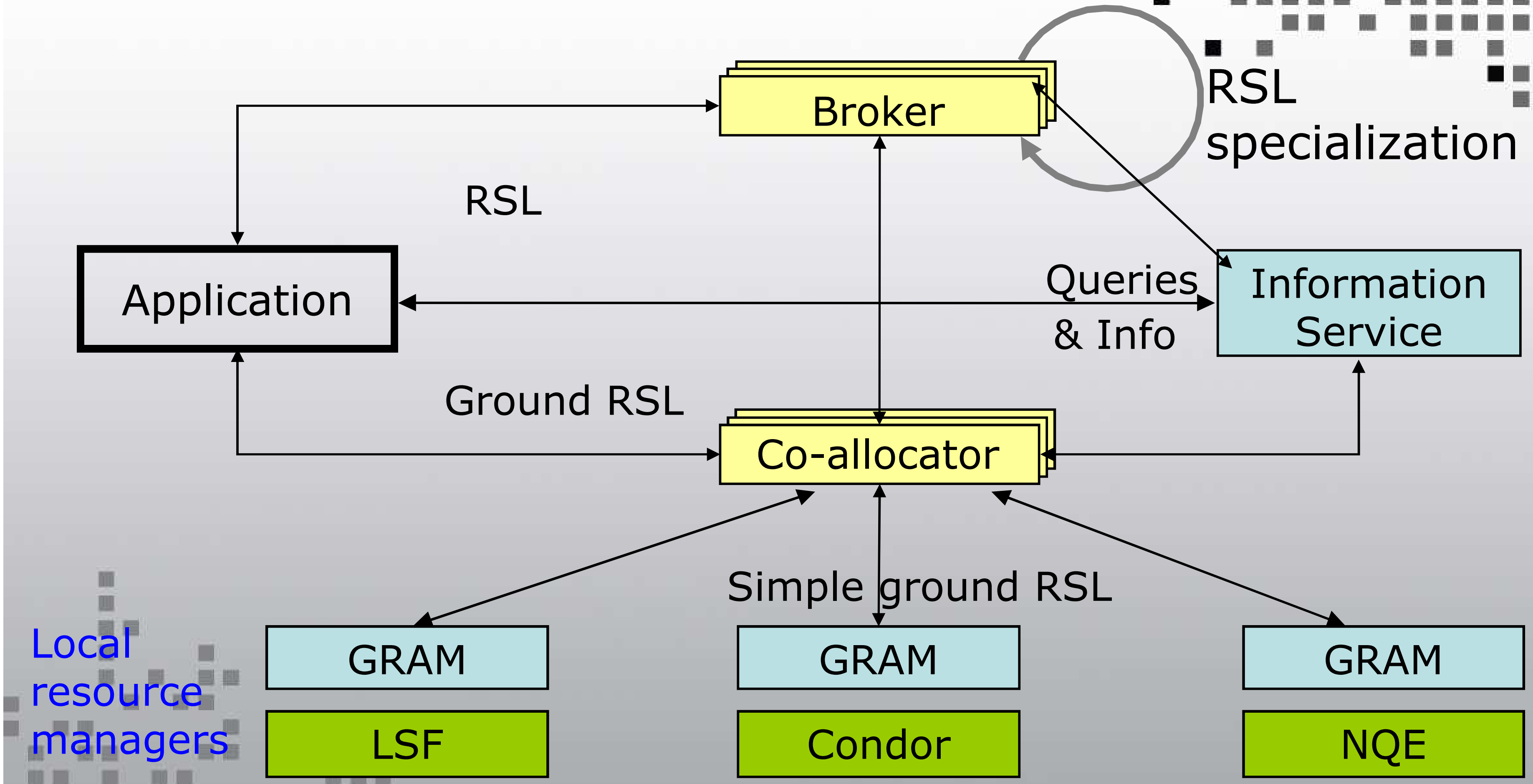
The Challenge

- Enabling secure, controlled remote access to heterogeneous computational resources and management of remote computation
  - Authentication and authorization
  - Resource discovery & characterization
  - Reservation and allocation
  - Computation monitoring and control
- Addressed by new protocols & services
  - GRAM protocol as a basic building block
  - Resource brokering & co-allocation services
  - GSI for security, MDS for discovery

Resource Management

- The **Grid Resource Allocation Management (GRAM)** protocol and client API allows programs to be started on remote resources, despite local heterogeneity
- **Resource Specification Language (RSL)** is used to communicate requirements
- A layered architecture allows application-specific resource brokers and co-allocators to be defined in terms of GRAM services
  - Integrated with Condor, PBS, MPICH-G2, …

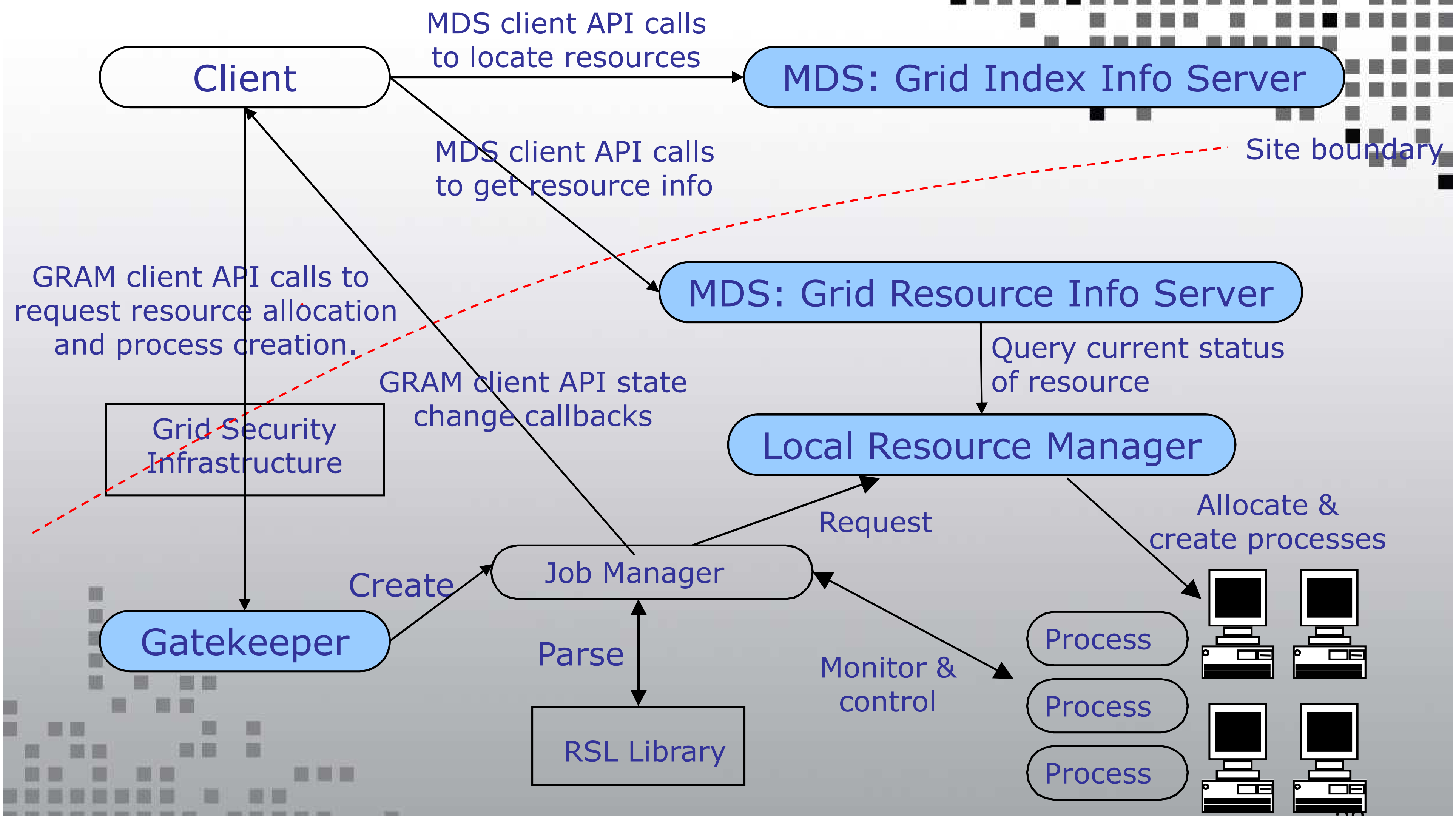
Resource Management Architecture



Globus Toolkit Implementation

- Gatekeeper
  - – Single point of entry
  - – Authenticates user, maps to local security environment, runs service
  - – In essence, a “secure inetd”
- Job manager
  - – A gatekeeper service
  - – Layers on top of local resource management system (e.g., PBS, LSF, etc.)
  - – Handles remote interaction with the job

GRAM Components


Client
MDS client API calls to locate resources
MDS: Grid Index Info Server
MDS client API calls to get resource info
Site boundary
GRAM client API calls to request resource allocation and process creation.
MDS: Grid Resource Info Server
Query current status of resource
GRAM client API state change callbacks
Grid Security Infrastructure
Local Resource Manager
Allocate & create processes
Request
Create
Job Manager
Gatekeeper
Parse
Monitor & control
Process
Process
Process
RSL Library

Job Submission Interfaces

- Globus Toolkit includes several command line programs for job submission
  - – globus-job-run: Interactive jobs
  - – globus-job-submit: Batch/offline jobs
  - – globusrun: Flexible scripting infrastructure
- Others are building better interfaces
  - – General purpose
    - Condor-G, PBS, GRD, Hotpage, etc
  - – Application specific
    - ECCE’, Cactus, Web portals

The Globus Toolkit™:
Information Services

The Globus Project™

Argonne National Laboratory
USC Information Sciences Institute

http://www.globus.org

Grid Information Services

- System information is critical to operation of the grid and construction of applications
  - What resources are available?
    - Resource discovery
  - What is the "state" of the grid?
    - Resource selection
  - How to optimize resource use
    - Application configuration and adaptation?
- We need a general information infrastructure to answer these questions

Examples of Useful Information

- Characteristics of a compute resource
  - IP address, software available, system administrator, networks connected to, OS version, load
- Characteristics of a network
  - Bandwidth and latency, protocols, logical topology
- Characteristics of the Globus infrastructure
  - Hosts, resource managers

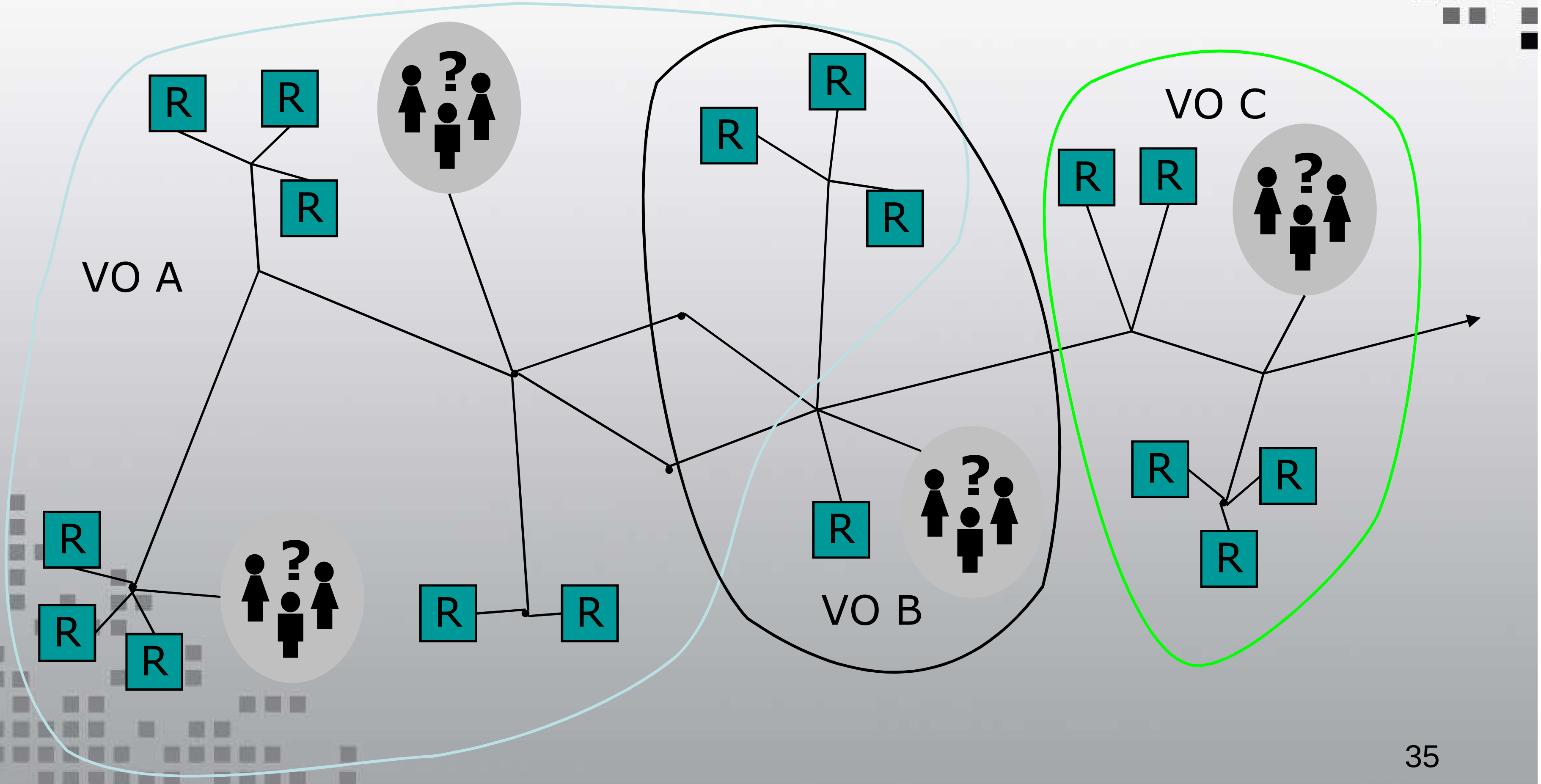
Grid Information: Facts of Life

- Information is always old
  - Time of flight, changing system state
  - Need to provide quality metrics
- Distributed state hard to obtain
  - Complexity of global snapshot
- Component will fail
- Scalability and overhead
- Many different usage scenarios
  - Heterogeneous policy, different information organizations, etc.

Grid Information Service

- Provide access to static and dynamic information regarding system components
- A basis for configuration and adaptation in heterogeneous, dynamic environments
- Requirements and characteristics
  - Uniform, flexible access to information
  - Scalable, efficient access to dynamic data
  - Access to multiple information sources
  - Decentralized maintenance

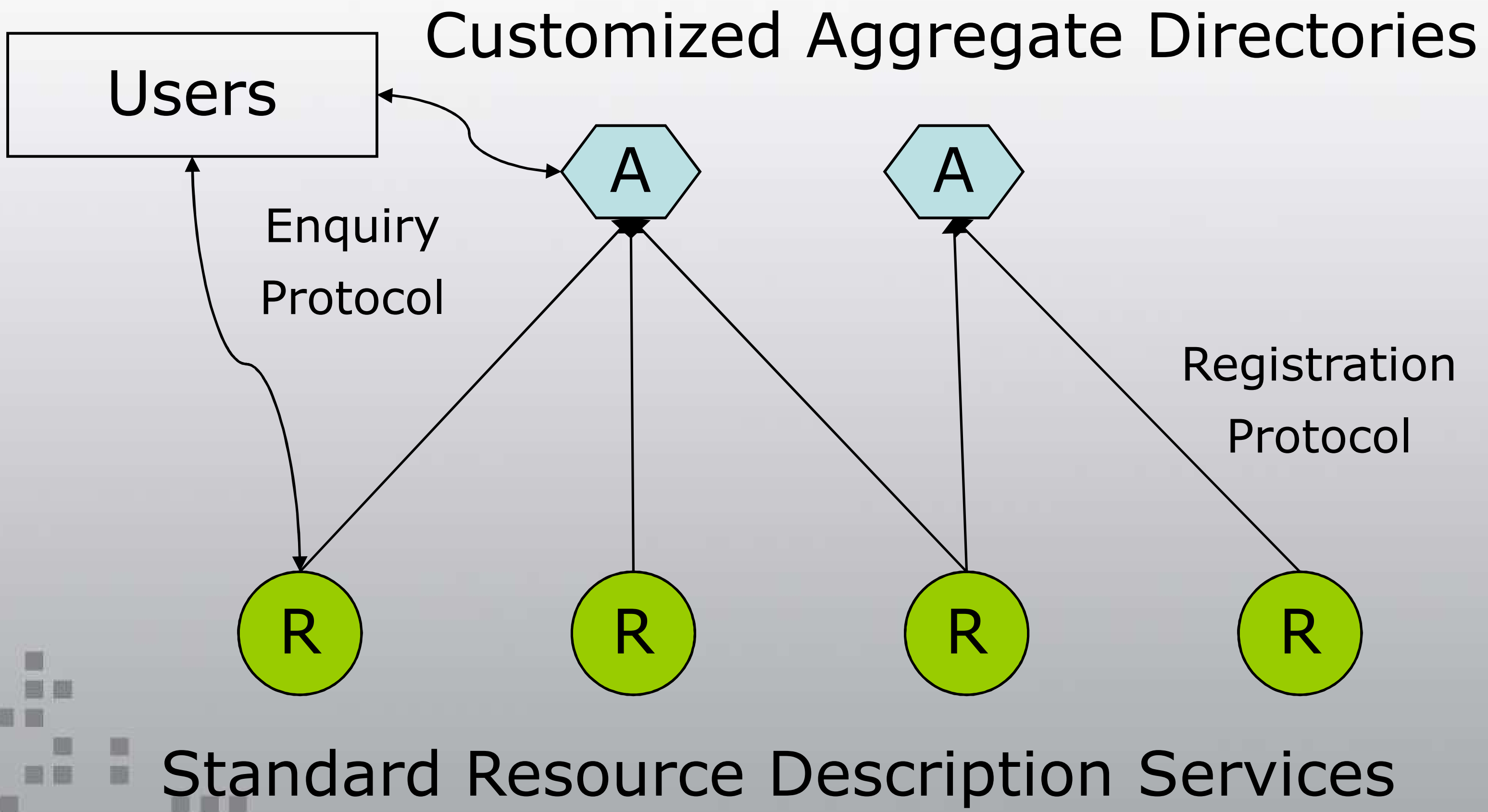
The GIS Problem: Many Information Sources, Many Views



Information Protocols

- Grid Resource Registration Protocol
  - – Support information/resource discovery
  - – Designed to support machine/network failure
- Grid Resource Inquiry Protocol
  - – Query resource description server for information
  - – Query aggregate server for information
  - – LDAP V3.0 in Globus 1.1.3

GIS Architecture


Customized Aggregate Directories
Users
A
A
Enquiry
Protocol
Registration
Protocol
R
R
R
R
Standard Resource Description Services

Metacomputing Directory Service

- Use LDAP as Inquiry
- Access information in a distributed directory
  - Directory represented by collection of LDAP servers
  - Each server optimized for particular function
- Directory can be updated by:
  - Information providers and tools
  - Applications (i.e., users)
  - Backend tools which generate info on demand
- Information dynamically available to tools and applications

Two Classes Of MDS Servers

- Grid Resource Information Service (GRIS)
  - Supplies information about a specific resource
  - Configurable to support multiple information providers
  - LDAP as inquiry protocol
- Grid Index Information Service (GIIS)
  - Supplies collection of information which was gathered from multiple GRIS servers
  - Supports efficient queries against information which is spread across multiple GRIS server
  - LDAP as inquiry protocol

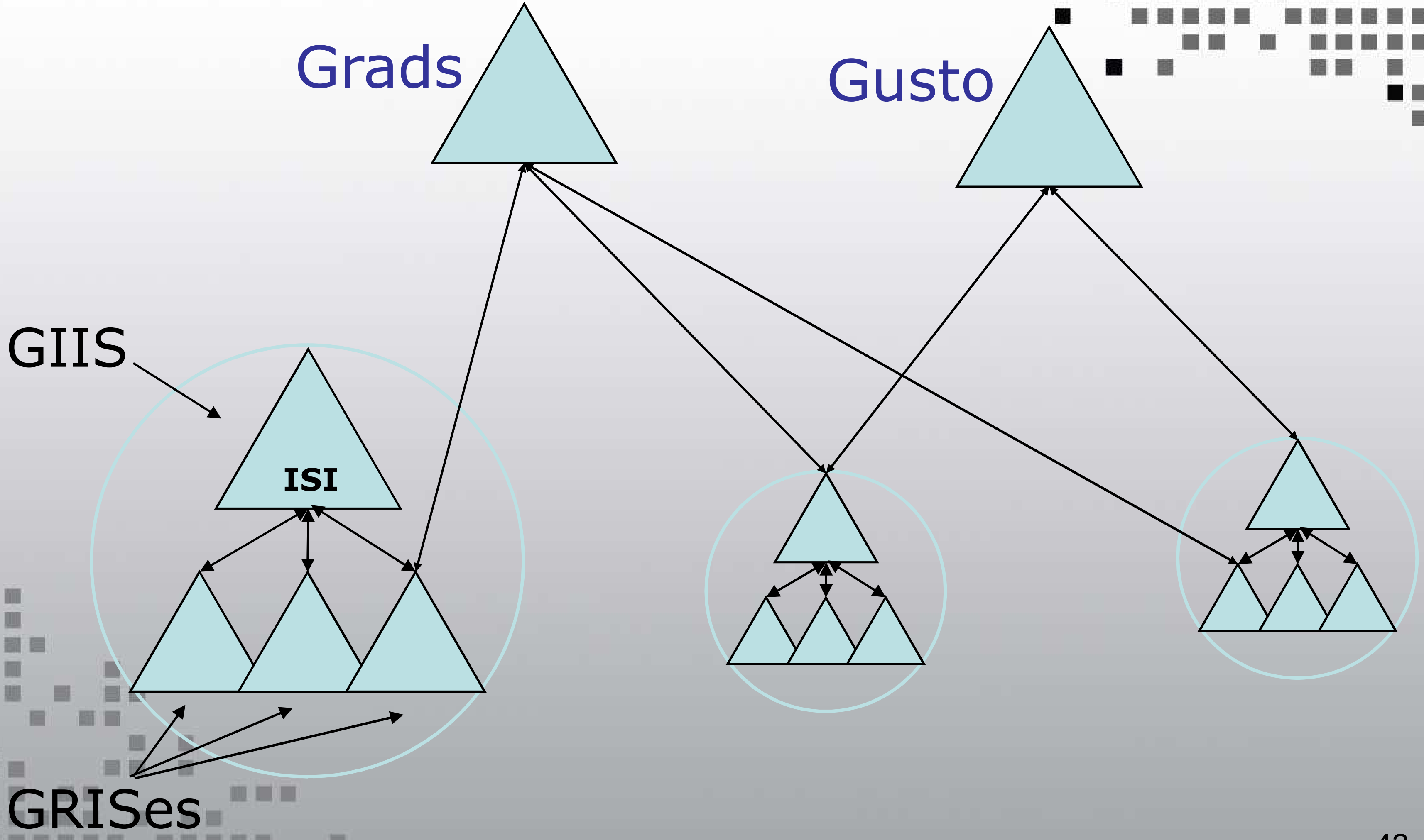
Grid Resource Information Service

- Server which runs on each resource
  - Given the resource DNS name, you can find the GRIS server (well known port = 2135)
- Provides resource specific information
  - Much of this information may be dynamic
    - Load, process information, storage information, etc.
    - GRIS gathers this information on demand
- "White pages" lookup of resource information
  - Ex: How much memory does machine have?
- "Yellow pages" lookup of resource options
  - Ex: Which queues on machine allows large jobs?

Grid Index Information Service

- GIIS describes a class of servers
  - Gathers information from multiple GRIS servers
  - Each GIIS is optimized for particular queries
    - Ex1: Which Alliance machines are >16 process SGIs?
    - Ex2: Which Alliance storage servers have >100Mbps bandwidth to host X?
  - Akin to web search engines
- Organization GIIS
  - The Globus Toolkit ships with one GIIS
  - Caches GRIS info with long update frequency
    - Useful for queries across an organization that rely on relatively static information (Ex1 above)
- Can be merged into GRIS

Logical MDS Deployment



Example: Discovering CPU Load

- Retrieve CPU load fields of computer resources

```
% grid-info-search -L “(objectclass=GlobusComputeResource)” \
                  dn cpuload1 cpuload5 cpuload15
```

```
dn: hn=lemon.mcs.anl.gov, ou=MCS, o=Argonne National Laboratory,
  o=Globus, c=US
cpuload1: 0.48
cpuload5: 0.20
cpuload15: 0.03

dn: hn=tuva.mcs.anl.gov, ou=MCS, o=Argonne National Laboratory,
 o=Globus, c=US
cpuload1: 3.11
cpuload5: 2.64
cpuload15: 2.57
```

The Globus Toolkit™:
Data Management Services

The Globus Project™

Argonne National Laboratory
USC Information Sciences Institute

http://www.globus.org

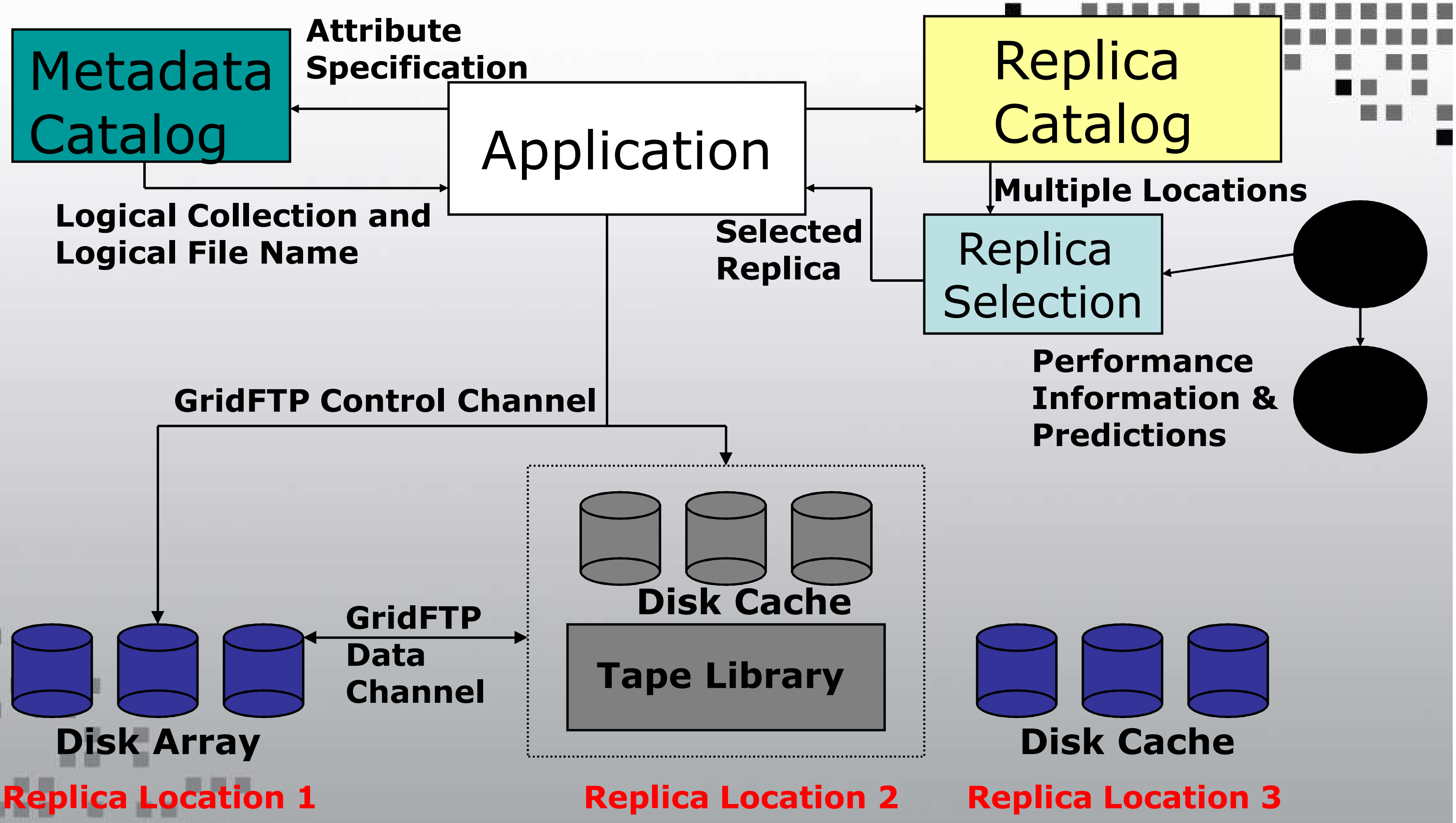
Data Intensive Issues Include…

- Harness [potentially large numbers of] data, storage, network resources located in distinct administrative domains
- Respect local and global policies governing what can be used for what
- Schedule resources efficiently, again subject to local and global constraints
- Achieve high performance, with respect to both speed and reliability.

Desired Data Grid Functionality

- High-speed, reliable access to remote data
- Automated discovery of “best” copy of data
- Manage replication to improve performance
- Co-schedule compute, storage, network
- “Transparency” wrt delivered performance
- Enforce access control on data
- Allow representation of “global” resource allocation policies

A Model Architecture for Data Grids



Globus Toolkit Components

Two major Data Grid components:

1. Data Transport and Access
   - Common protocol
     - Secure, efficient, flexible, extensible data movement
   - Family of tools supporting this protocol

2. Replica Management Architecture
   - Simple scheme for managing:
     - multiple copies of files
     - collections of files

And The Protocol Is … GridFTP

- Why FTP?
  - Ubiquity enables interoperation with many commodity tools
  - Already supports many desired features, easily extended to support others
  - Well understood and supported
- We use the term GridFTP to refer to
  - Transfer protocol which meets requirements
  - Family of tools which implement the protocol
- Note GridFTP > FTP
- Note that despite name, GridFTP is not restricted to file transfer!

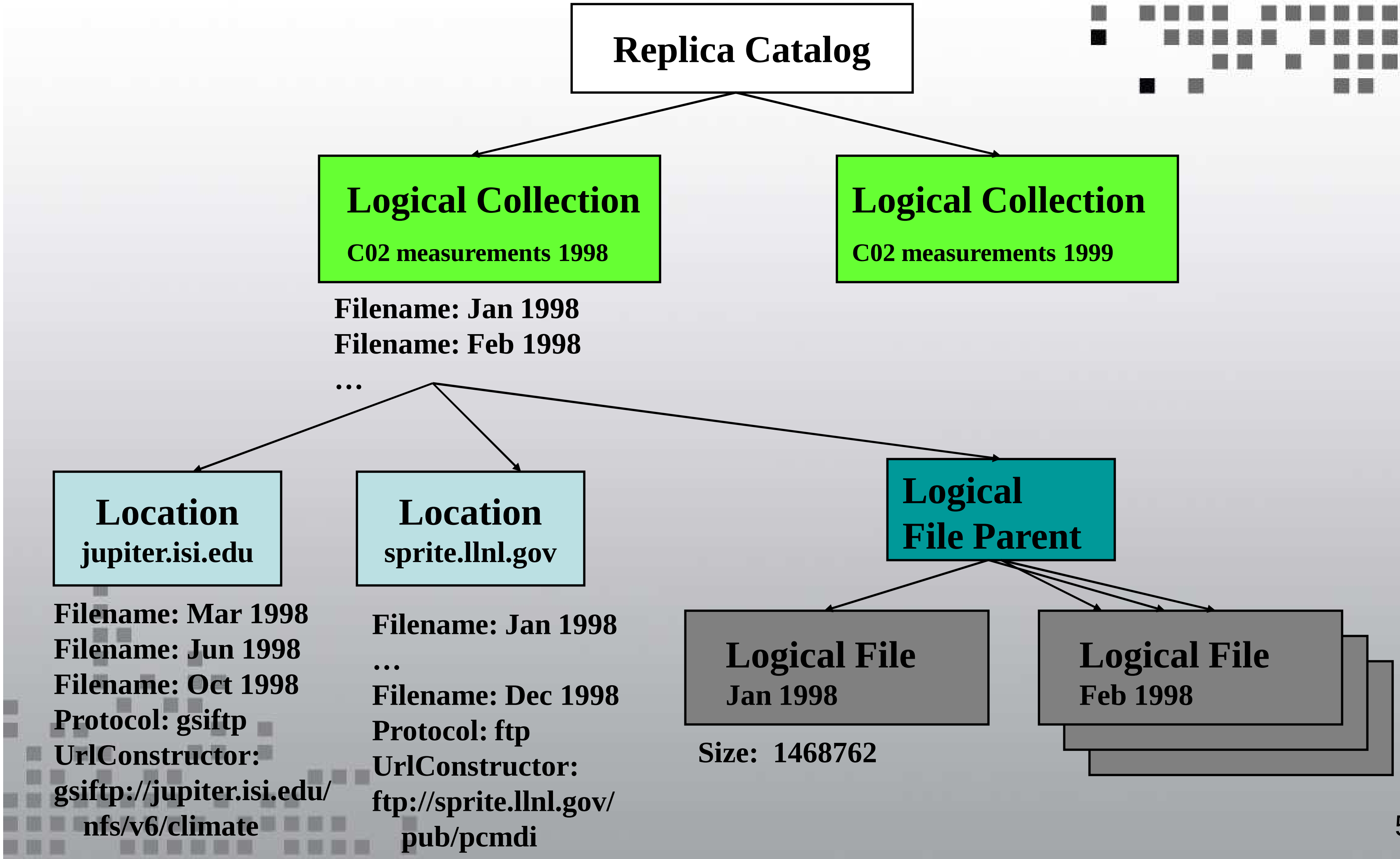
GridFTP: Basic Approach

- FTP protocol is defined by several IETF RFCs
- Start with most commonly used subset
  - Standard FTP: get/put etc., 3rd-party transfer
- Implement standard but often unused features
  - GSS binding, extended directory listing, simple restart
- Extend in various ways, while preserving interoperability with existing servers
  - Striped/parallel data channels, partial file, automatic & manual TCP buffer setting, progress monitoring, extended restart

Replica Management

- Maintain a mapping between logical names for files and collections at one or more physical locations
- Important for many applications
  - Example: CERN HLT data
    - Multiple petabytes of data per year
    - Copy of everything at CERN (Tier 0)
    - Subsets at national centers (Tier 1)
    - Smaller regional centers (Tier 2)
    - Individual researchers will have copies

Replica Catalog Structure: A Climate Modeling Example



Replica Catalog

Logical Collection

C02 measurements 1998

Logical Collection

C02 measurements 1999

Filename: Jan 1998
Filename: Feb 1998
…

Location

jupiter.isi.edu

Filename: Mar 1998
Filename: Jun 1998
Filename: Oct 1998
Protocol: gsiftp
UrlConstructor:
gsiftp://jupiter.isi.edu/
nfs/v6/climate

Location

sprite.llnl.gov

Filename: Jan 1998
…
Filename: Dec 1998
Protocol: ftp
UrlConstructor:
ftp://sprite.llnl.gov/
pub/pcmdi

Logical
File Parent

Logical File

Jan 1998

Size: 1468762

Logical File

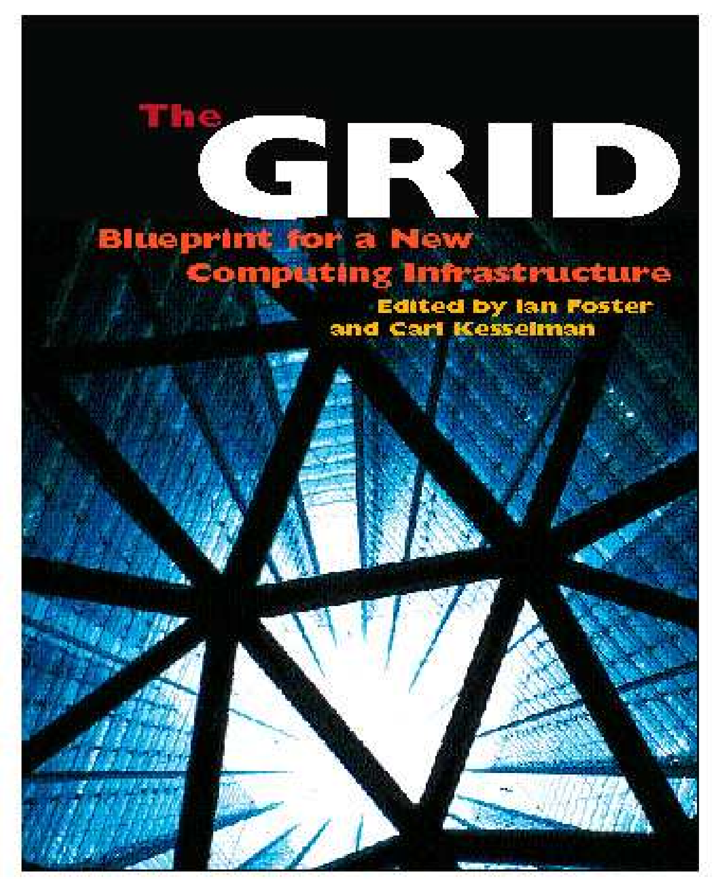
Feb 1998

Replica Catalog Services as Building Blocks: Examples

- Combine with information service to build replica selection services
  - E.g. “find best replica” using performance info from NWS and MDS
  - Use of LDAP as common protocol for info and replica services makes this easier
- Combine with application managers to build data distribution services
  - E.g., build new replicas in response to frequent accesses

For More Information

- Globus Project™
  - www.globus.org
- Grid Forum
  - www.gridforum.org
- Book (Morgan Kaufman)
  - www.mkp.com/grids


The GRID
Blueprint for a New Computing Infrastructure
Edited by Ian Foster and Carl Kesselman