Globus Toolkit Implementation

Charles Bacon

Argonne National Laboratory

University of Chicago

Overview

- Security for VOs
- Data Services
  - GridFTP, RFT, RLS, OGSA-DAI
- Execution Services
  - WS GRAM, Workspace Service
- Information Services
  - Index Service, Information Providers, WebMDS
- Security Services
  - MyProxy, GSI-OpenSSH, CAS

Security for Virtual Organizations

- The Grid Security Infrastructure (GSI) provides for the requirements of Virtual Organizations:
  - Single sign-on
  - Delegation of rights
  - Mutual Authentication
- Based on X.509 Public Key Infrastructure plus RFC 3820 *proxy certificates*

Certificates

- Every user and service is identified by a certificate
- Contains:
  - A subject name
  - A public key
  - The identity of a Certificate Authority
  - The digital signature of the named CA
- The signature creates the link between the public key and the subject name

Authentication and Authorization

- To authenticate, you present your proxy certificate for validation
- This establishes your Distinguished Name
- The DN can then be mapped to a level of authorization
  - Can be accomplished via a callout to your authorization system of choice
- The resource owner has the final word

Data Services

- The GridFTP protocol provides for the secure, robust, fast and efficient transfer of (especially bulk) data
- The Reliable File Transfer service provides scheduler-like functionality for data movement
- The Replica Location Service is a distributed registry that keeps track of where replicas exist on physical storage systems

GridFTP

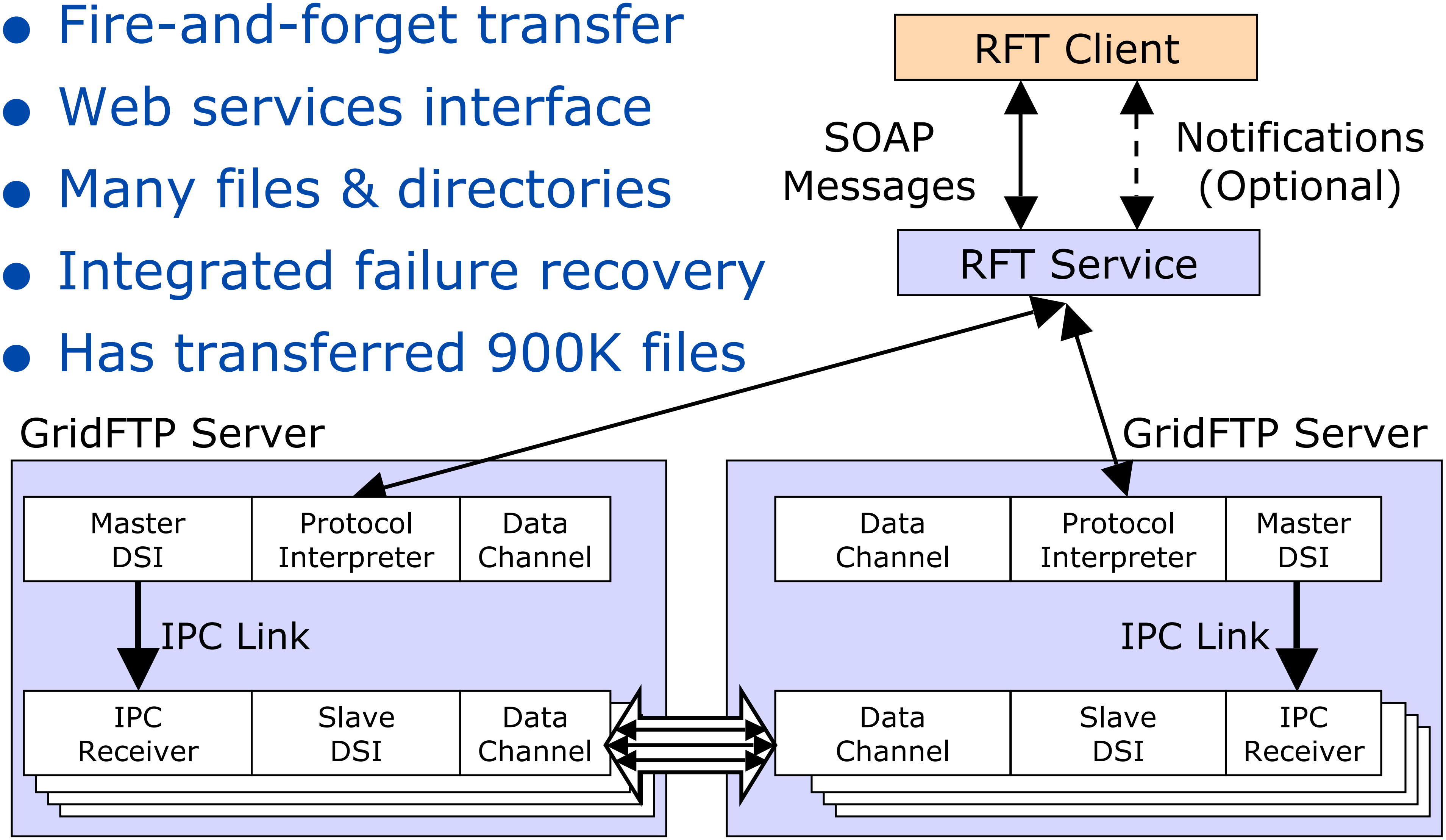
- GT4 includes a server implementation of the GridFTP protocol, called `globus-gridftp-server`
- A commandline client, `globus-url-copy`
- Pluggable Data Storage Interfaces (DSI) for SRB, HPSS, NeST
- Striped data-nodes for higher bandwidth

Reliable File Transfer Service

- Provides a Web Service interface to GridFTP file transfers
- Provide a list of source and destination URLs, and they will be transferred
- Can subscribe for notifications of state change events
- State stored in a database for fault tolerance

Reliable File Transfer: Third Party Transfer

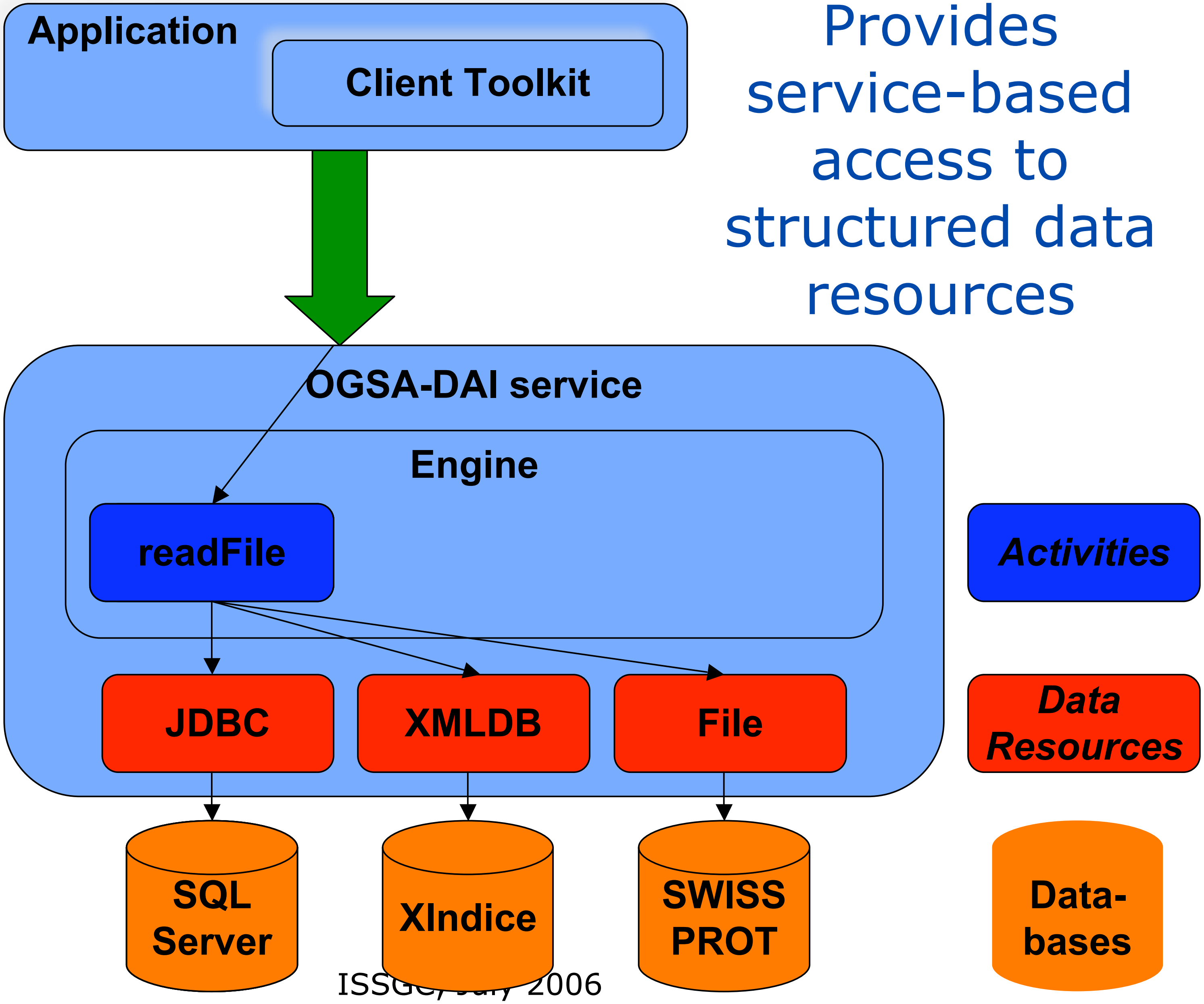
- Fire-and-forget transfer
- Web services interface
- Many files & directories
- Integrated failure recovery
- Has transferred 900K files



Replica Location Service

- Maps Logical File Names (LFN) to one or more Physical File Names (PFN)
- Distributed registries allow for scaling and fault tolerance
- The Data Replication Service combines RFT and RLS to ensure that a specified set of files exists on a storage site

The OGSA-DAI Framework



Provides service-based access to structured data resources

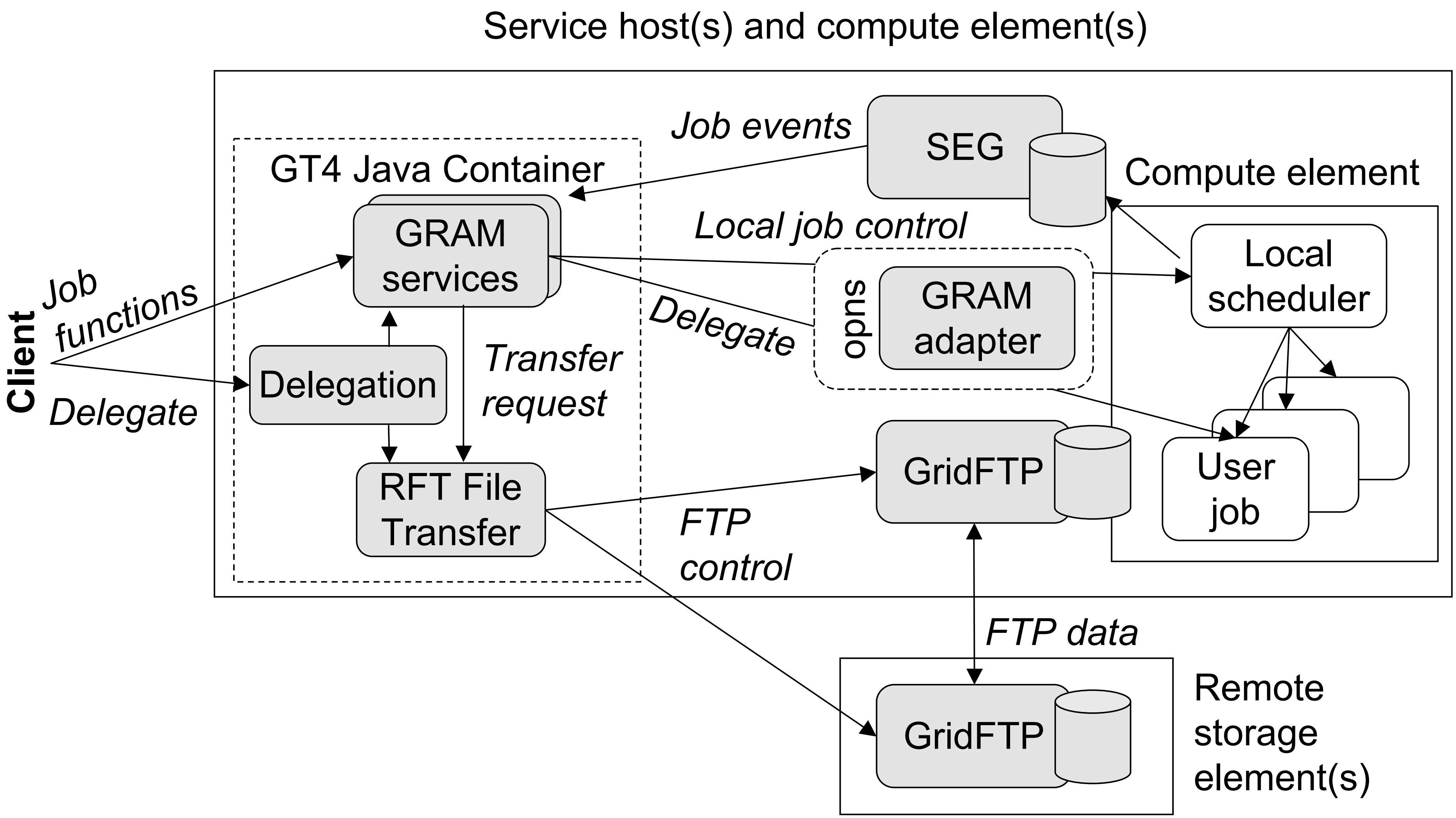
OGSA-DAI Hides Heterogeneity

- Supports data access, insert and update
  - Relational: MySQL, Oracle, DB2, SQL Server, Postgres
  - XML: Xindice, eXist
  - Files – CSV, BinX, EMBL, OMIM, SWISSPROT,…
- Supports data delivery
  - SOAP over HTTP
  - FTP; GridFTP
  - E-mail
  - Inter-service
- Supports data transformation
  - XSLT
  - ZIP; GZIP
- Supports security
  - X.509 certificate based security

Execution Services

- Grid Resource Access Management (GRAM) is intended for jobs where arbitrary programs, stateful monitoring, credential management, and file staging are important
- It manages this via a Service Oriented Architecture

GT4 WS GRAM Architecture



WS-GRAM Approach: Execution

- At the most basic level: Create a WSRF resource for your Job
- GRAM is an engine for communicating with a range of different local resource schedulers using a standard message format
- The GRAM service itself is a job management service that represents, monitors, and controls the overall job life cycle

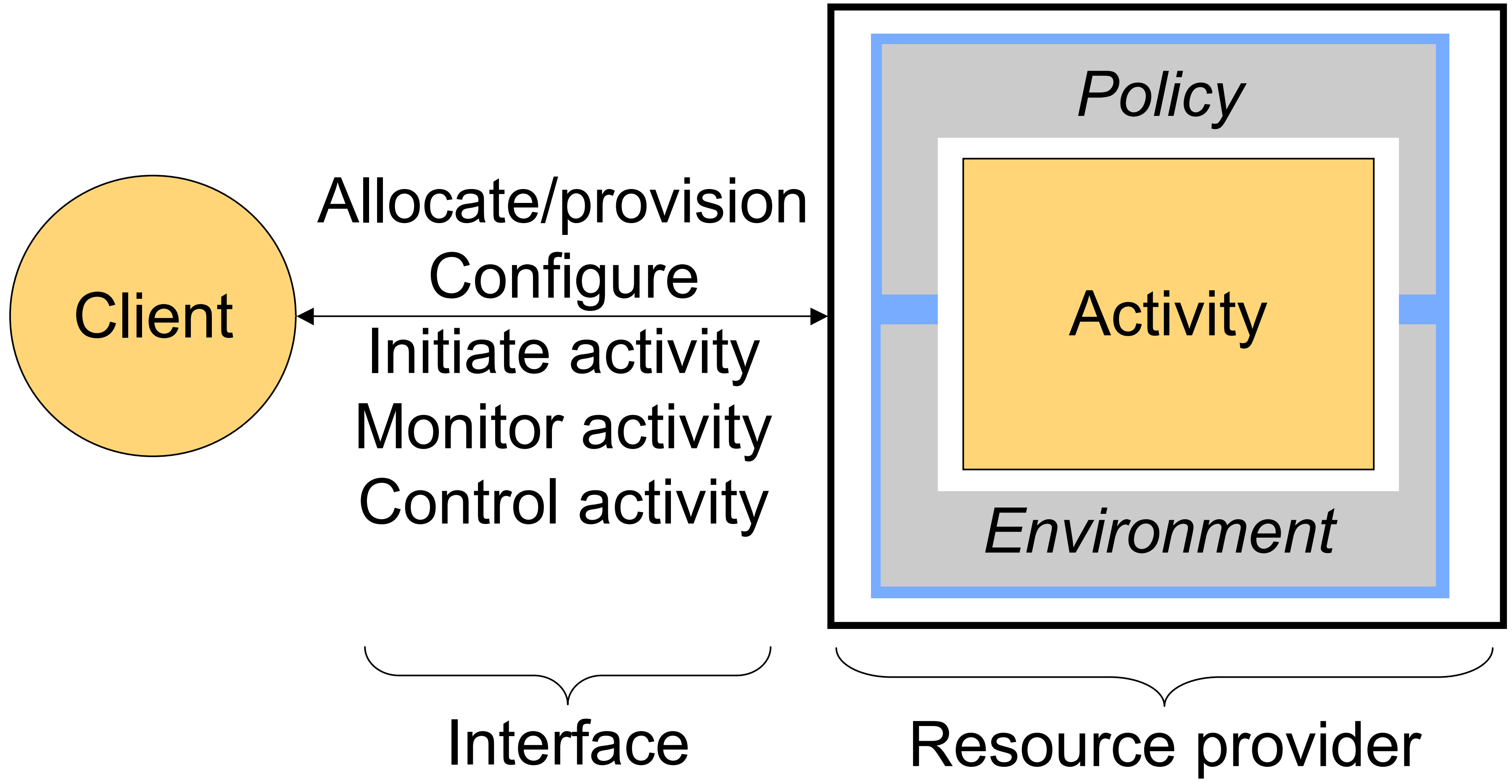
WS-GRAM Approach: Data

- File transfer services support staging of files into and out of compute resources
- Uses the RFT service to provide reliable, high-performance transfers of files between the compute resource and external (gridftp) data storage elements before and after the job execution
- Allows an arbitrary number of files to stage in/out, not just stdout/stderr

WS-GRAM Approach: Security

- The Delegation Service provides a WSRF interface to the delegation of proxy credentials
- Lets you delegate multiple credentials so your job can coordinate cross-VO activities
- Also allows for credential refresh for long-running jobs
- Can reduce the overhead for submission of a large number of small jobs

Workspace Service: The Hosted Activity



Monitoring and Discovery

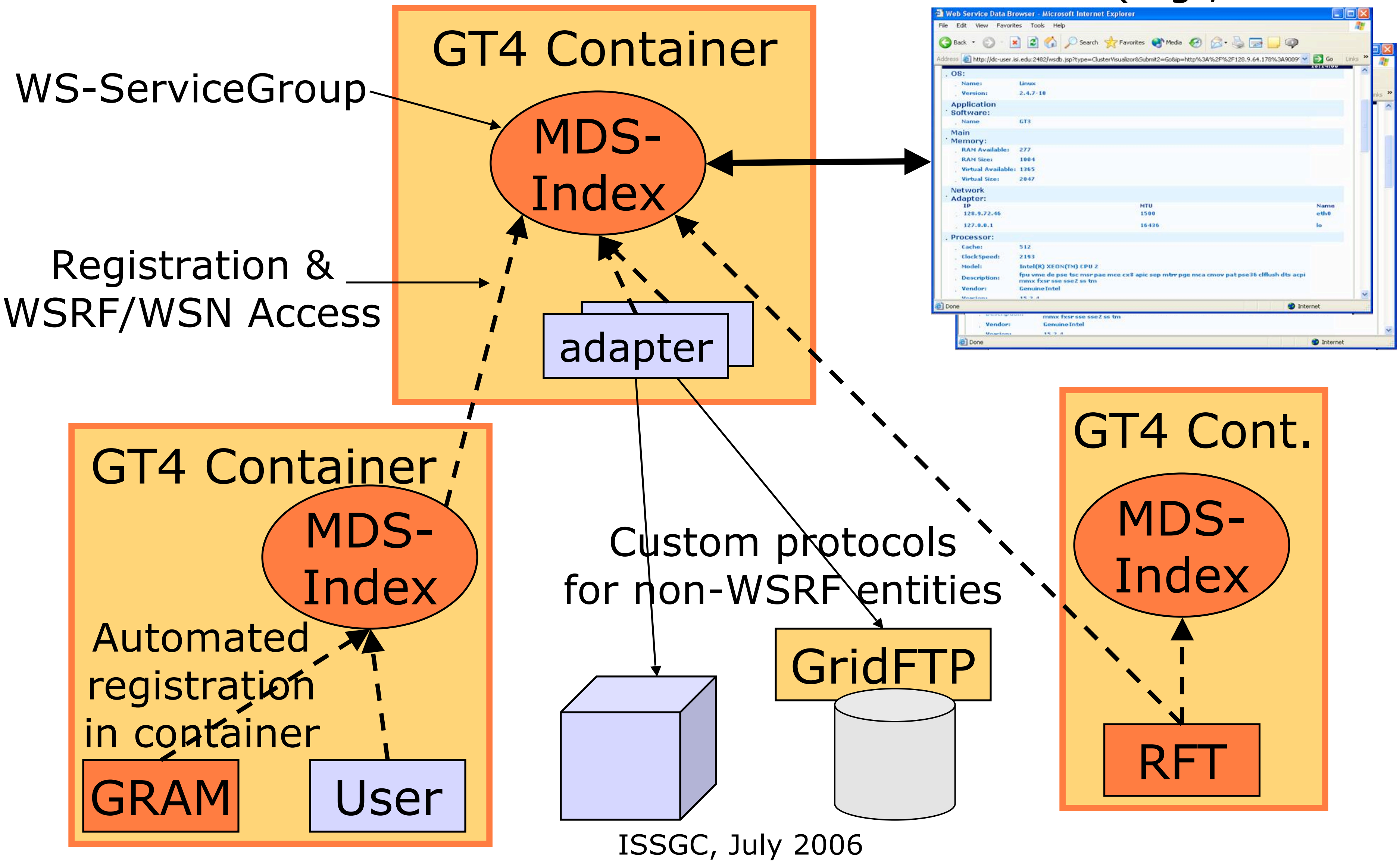
- "Every service should be monitorable and discoverable using common mechanisms"
  - WSRF/WSN provides those mechanisms
- A common aggregator framework for collecting information from services, thus:
  - MDS-Index: Xpath queries, with caching
  - MDS-Trigger: perform action on condition
- Deep integration with Globus containers & services: every GT4 service is discoverable
  - GRAM, RFT, GridFTP, CAS, …

Information Services

- Index service collects data from various sources and provides a query/subscription interface to that data
- Trigger service collects data from various sources and can be configured to take action based on that data
- WebMDS is a web-based interface to WSRF resource property information that is available as a user-friendly front-end to the Index Service

GT4 Monitoring & Discovery

Clients (e.g., WebMDS)



WS-ServiceGroup

Registration & WSRF/WSN Access

GT4 Container

MDS-Index

adapter

GT4 Container

MDS-Index

Automated registration in container

GRAM

User

Custom protocols for non-WSRF entities

GridFTP

GT4 Cont.

MDS-Index

RFT

Web Service Data Browser - Microsoft Internet Explorer

Address http://dc-user.isi.edu:2482/wsdb.jsp?type=ClusterVisualizor&Submit2=Go&ip=http%3A%2F%2F128.9.64.178%3A9009

OS:

Name:	Linux
Version:	2.4.7-10

Application Software:

Name	GT3

Main Memory:

RAM Available:	277
RAM Size:	1004
Virtual Available:	1365
Virtual Size:	2047

Network Adapter:

IP	MTU	Name
128.9.72.46	1500	eth0
127.0.0.1	16436	lo

Processor:

Cache:	512
ClockSpeed:	2193
Model:	Intel(R) XEON(TM) CPU 2
Description:	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss tm
Vendor:	GenuineIntel

Done

Internet

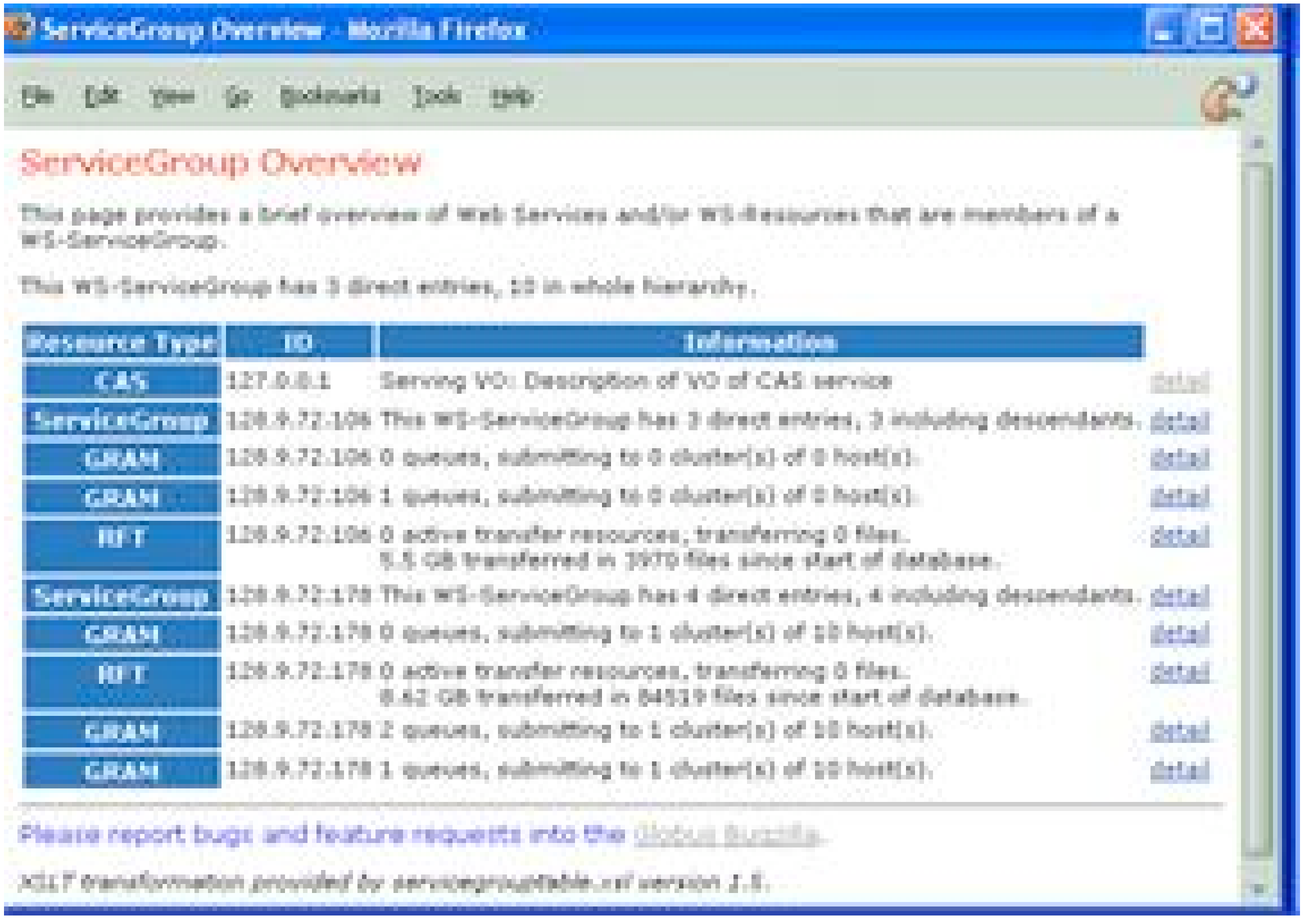
Index Service

- Each Globus container that has MDS4 installed will automatically have a default Index Service instance
- By default, the local services register into that index
- Can aggregate index services into a central VO-level index service

Information Providers

- Information Providers gather information from external sources and publish it as WSRF Resource Properties
- Allows cluster monitoring systems like Ganglia and Hawkeye to publish information in the GLUE Schema
- Also publish queue data for SGE, LSF, OpenPBS, PBSPro, Torque

WebMDS



ServiceGroup Overview - Mozilla Firefox
File Edit View Go Bookmarks Tools Help

ServiceGroup Overview

This page provides a brief overview of Web Services and/or WS-Resources that are members of a WS-ServiceGroup.

This WS-ServiceGroup has 3 direct entries, 10 in whole hierarchy.

Resource Type	ID	Information	
CAS	127.0.0.1	Serving VO: Description of VO of CAS service	detail
ServiceGroup	128.9.72.106	This WS-ServiceGroup has 3 direct entries, 3 including descendants.	detail
GRAM	128.9.72.106	0 queues, submitting to 0 cluster(s) of 0 host(s).	detail
GRAM	128.9.72.106	1 queues, submitting to 0 cluster(s) of 0 host(s).	detail
RFT	128.9.72.106	0 active transfer resources, transferring 0 files. 5.5 GB transferred in 3970 files since start of database.	detail
ServiceGroup	128.9.72.178	This WS-ServiceGroup has 4 direct entries, 4 including descendants.	detail
GRAM	128.9.72.178	0 queues, submitting to 1 cluster(s) of 10 host(s).	detail
RFT	128.9.72.178	0 active transfer resources, transferring 0 files. 8.42 GB transferred in 84519 files since start of database.	detail
GRAM	128.9.72.178	2 queues, submitting to 1 cluster(s) of 10 host(s).	detail
GRAM	128.9.72.178	1 queues, submitting to 1 cluster(s) of 10 host(s).	detail

Please report bugs and feature requests into the Globus Bugzilla.

XSLT transformation provided by servicegrouptable.xsl version 1.5.

Security Services

- Delegation Service (as seen in WS GRAM)
- SimpleCA for creating/running a small Certificate Authority
- GSI-OpenSSH for GSI security with SSH
- MyProxy server for credential management

GSI-OpenSSH

- GSI-OpenSSH can be used to login to remote systems and transfer files between systems without entering a password
- Automatically delegates a proxy credential to the remote system

MyProxy

- You can store X.509 proxy credentials in the MyProxy repository, protected by a passphrase for later retrieval over the network
- MyProxy can also be used for authentication to grid portals and credential renewal with job managers

Community Authorization Service

- A CAS server issues assertions to the virtual organization users, granting them fine-grained access rights to resources
- Servers recognize and enforce the assertions
- CAS is designed to be extensible to multiple services and is currently supported by the GridFTP server