Infrastructure Systems: The Globus Toolkit

BRIITE Meeting - Nov 2-4, 2005

2-4 Nov 2005, Salk Institute, La Jolla, CA

Frank Siebenlist
(Globus Alliance / Argonne National Laboratory / University of Chicago)
franks@mcs.anl.gov - http://www.globus.org/
Outline

- Globus Alliance
- Grids
- Globus Toolkit Introduction
- Virtual Organizations
- GT’s BIG Security “Issue”
- Questions & Discussion
The Globus Alliance
Making Grid computing a reality

- Close collaboration with real Grid projects in science and industry
- Development and promotion of standard Grid protocols (e.g. OGSA) to enable interoperability and shared infrastructure
- Development and promotion of standard Grid software APIs and SDKs to enable portability and code sharing
- The Globus Toolkit®: Open source, reference software base for building Grid infrastructure and applications
- Global Grid Forum: Development of standard protocols and APIs for Grid computing
How Globus Works

- **Globus** is a distributed open source community with many contributors & users
  - CVS, documentation, bugzilla, email lists
  - Modular structure allows many to contribute
- **Globus Alliance Board** provides governance when needed
  - Meritocracy: individuals who demonstrate ongoing contributions & commitment
  - Primarily: what to include, when to release
- **Globus Alliance** is an informal partnership of organizations led by Board members
On April 29, 2005 the Globus Alliance released the finest version of the Globus Toolkit to date!

GT-4.0
The Application-Infrastructure Gap

Dynamic and/or Distributed Applications
The Application-Infrastructure Gap

Dynamic and/or Distributed Applications

Shared Distributed Infrastructure
Bridging the Gap: Grid Infrastructure

- Service-oriented **applications**
  - Wrap applications as services
  - Compose applications into workflows
Bridging the Gap: Grid Infrastructure

- **Service-oriented applications**
  - Wrap applications as services
  - Compose applications into workflows

- **Service-oriented Grid infrastructure**
  - Provision physical resources to support application workloads

Users ➔ Composition ➔ Workflows ➔ Invocation

Provisioning

Appln Service ➔ Appln Service

Appln Service ➔ Appln Service

Appln Service ➔ Appln Service

Appln Service ➔ Appln Service
Globus is Grid Infrastructure

- Software for Grid infrastructure
  - Service enable new & existing resources
  - E.g., GRAM on computer, GridFTP on storage system, custom application service
  - Uniform abstractions & mechanisms
- Tools to build applications that exploit Grid infrastructure
  - Registries, security, data management, ...
- Open source & open standards
  - Each empowers the other
- Enabler of a rich tool & service ecosystem
Globus as Service-Oriented Infrastructure

User Application

User Application

User Application

Computers

Specialized resource

Storage

Database
Globus as Service-Oriented Infrastructure

Uniform interfaces, security mechanisms, Web service transport, monitoring

User Application Tool

User Application

User Application Tool

Reliable File Transfer

User Svc

Host Env

MyProxy

DAIS

Computers

Specialized resource

Storage

GridFTP

GRAM

MDS-Index

Database

Nov 3, 2005
A Typical eScience Use of Globus: Network for Earthquake Eng. Simulation

Links instruments, data, computers, people
A Typical eScience Use of Globus: Network for Earthquake Eng. Simulation

Links instruments, data, computers, people
There is a "bunch crossing" every 25 nsecs. There are 100 "triggers" per second. Each triggered event is ~1 MByte in size.

Each institute will have ~10 physicists working on one or more channels; data for these channels should be cached by the institute server.
Global Community

Open Science Grid

Building the National Virtual Collaboratory for Earthquake Engineering.

CERN

Data Grid

Access Grid

grid.it project

Grid Ireland

NGriD

NEESgrid

Grid3

DataTAG

APGrid

NAREGI

GridLab
Globus Toolkit

- Core Web services
  - Infrastructure for building new services
- Security
  - Apply uniform policy across distinct systems
- Execution management
  - Provision, deploy, & manage services
- Data management
  - Discover, transfer, & access large data
- Monitoring
  - Discover & monitor dynamic services
WSRF & WS-Notification

- Naming and bindings (basis for virtualization)
  - Every resource can be uniquely referenced, and has one or more associated services for interacting with it
- Lifecycle (basis for fault resilient state management)
  - Resources created by services following factory pattern
  - Resources destroyed immediately or scheduled
- Information model (basis for monitoring & discovery)
  - Resource properties associated with resources
  - Operations for querying and setting this info
  - Asynchronous notification of changes to properties
- Service Groups (basis for registries & collective svcs)
  - Group membership rules & membership management
- Base Fault type
GT4 Components

**CLIENT**
- Your Java Client
- Your C Client
- Your Python Client

**SERVER**
- Your Java Service
- GRAM
- RFT
- Delegation
- Index
- Trigger
- Archiver
- CAS
- OGSA-DAI
- GTCP

**Java Services in Apache Axis**
- Interoperable WS-I-compliant SOAP messaging

**Python hosting, GT Libraries**
- X.509 credentials = common authentication
- pyGlobus WS Core
- C WS Core

**C Services using GT Libraries and Handlers**
- GridFTP
- SimpleCA
- MyProxy
- RLS
- Pre-WS GRAM
- Pre-WS MDS

Nov 3, 2005

BRIITE Meeting: The Globus Toolkit
Our Goals for GT4

- **Usability, reliability, scalability, ...**
  - Web service components have quality equal or superior to pre-WS components
  - Documentation at acceptable quality level
- **Consistency with latest standards (WS-*, WSRF, WS-N, etc.) and Apache platform**
  - WS-I Basic Profile compliant
  - WS-I Basic Security Profile compliant
- **New components, platforms, languages**
  - And links to larger Globus ecosystem
GT4 Common Runtime

- Python WS Core
- C WS Core
- Java WS Core
- C Common Libraries
- eXtensible IO (XIO)
- Common Runtime
GT4 Web Services Core

User Applications

Custom WSRF Web Services

GT4 WSRF Web Services

WS-Addressing, WSRF, WS-Notification

WSDL, SOAP, WS-Security

GT4 Container

Custom Web Services

Registry Administration
GT4 Web Services Core

- Supports both GT (GRAM, RFT, Delegation, etc.) & user-developed services
- Redesign to enhance scalability, modularity, performance, usability
- Leverages existing WS standards
  - WS-I Basic Profile: WSDL, SOAP, etc.
  - WS-Security, WS-Addressing
- Adds support for emerging WS standards
  - WS-Resource Framework, WS-Notification
- Java, Python, & C hosting environments
  - Java is standard Apache
WSRF & WS-Notification

- **Naming and bindings** *(basis for virtualization)*
  - Every resource can be *uniquely referenced*, and has one or more *associated services* for interacting with it

- **Lifecycle** *(basis for fault resilient state mgmt)*
  - Resources created by services following *factory* pattern
  - Resources destroyed *immediately* or *scheduled*

- **Information model** *(basis for monitoring, discovery)*
  - Resource properties associated with resources
  - Operations for *querying* and *setting* this info
  - Asynchronous *notification* of changes to properties

- **Service groups** *(basis for registries, collective svcs)*
  - Group membership rules & membership management

- **Base Fault type**
GT4 Security

- Delegation
- Community Authorization
- Authentication Authorization
- Pre-WS Authentication Authorization
- Credential Mgmt
- Security
Globus Security

- Control access to shared services
  - Address autonomous management, e.g., different policy in different work-groups
- Support multi-user collaborations
  - Federate through mutually trusted services
  - Local policy authorities rule
- Allow users and application communities to set up dynamic trust domains
  - Personal/VO collection of resources working together based on trust of user/VO
GT4 Security

- Public-key-based authentication
- Extensible authorization framework based on Web services standards
  - SAML-based authorization callout
    - As specified in GGF OGSA-Authz WG
  - Integrated policy decision engine
    - XACML policy language, per-operation policies, pluggable
- Credential management service
  - MyProxy (One time password support)
- Community Authorization Service
- Standalone Delegation Service
GT4’s Use of Security Standards

<table>
<thead>
<tr>
<th>Authorization</th>
<th>Delegation</th>
<th>Authentication</th>
<th>Message Protection</th>
<th>Message format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML and grid-mapfile</td>
<td>grid-mapfile</td>
<td>SAML and grid-mapfile</td>
<td></td>
<td>SOAP</td>
</tr>
<tr>
<td>X.509 Proxy Certificates/ WS-Trust</td>
<td>Username/Password</td>
<td>X.509 Proxy Certificates/ WS-Trust</td>
<td></td>
<td>SOAP</td>
</tr>
<tr>
<td>X.509 End Entity Certificates</td>
<td>WS-Security</td>
<td>X.509 End Entity Certificates</td>
<td></td>
<td>SOAP</td>
</tr>
<tr>
<td>WS-SecureConversation</td>
<td>WS-Security</td>
<td>TLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOAP</td>
<td>SOAP</td>
<td>SOAP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Supported, but slow
- Supported, but insecure
- Fastest, so default
GT-XACML Integration

- eXtensible Access Control Markup Language
  - OASIS standard, open source implementations
- XACML: sophisticated policy language
- Globus Toolkit ships with XACML runtime
  - Included in every client and server built on GT
  - Turned-on through configuration
- ... that can be called transparently from runtime and/or explicitly from application ...
- ... and we use the XACML-“model” for our Authz Processing Framework
Other Security Services Include ...

- **MyProxy**
  - Simplified credential management
  - Web portal integration
  - Single-sign-on support
- **KCA & kx.509**
  - Bridging into/out-of Kerberos domains
- **SimpleCA**
  - Online credential generation
- **PERMIS**
  - Authorization service callout
GT4 Data Management

- Data Replication
- Data Access & Integration
  - Reliable File Transfer
- GridFTP
- Replica Location
- Data Mgmt
GT4 Data Management

- **Stage/move** large data to/from nodes
  - GridFTP, Reliable File Transfer (RFT)
  - Alone, and integrated with GRAM
- **Locate** data of interest
  - Replica Location Service (RLS)
- **Replicate** data for performance/reliability
  - Distributed Replication Service (DRS)
- **Provide access** to diverse data sources
  - File systems, parallel file systems, hierarchical storage: GridFTP
  - Databases: OGSA DAI
GridFTP in GT4

- 100% Globus code
  - No licensing issues
  - Stable, extensible
- IPv6 Support
- XIO for different transports
- Striping → multi-Gb/sec wide area transport
  - 27 Gbit/s on 30 Gbit/s link
- Pluggable
  - Front-end: e.g., future WS control channel
  - Back-end: e.g., HPSS, cluster file systems
  - Transfer: e.g., UDP, NetBLT transport
Reliable File Transfer: Third Party Transfer

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

GridFTP Server

RFT Client

RFT Service

SOAP Messages

Notifications (Optional)

Data Channel

Protocol Interpreter

Master DSI

Slave DSI

Data Channel

IPC Receiver

IPC Link
Replica Location Service

- Identify location of files via logical to physical name map
- Distributed indexing of names, fault tolerant update protocols
- GT4 version scalable & stable
- Managing ~40 million files across ~10 sites

<table>
<thead>
<tr>
<th>Local DB</th>
<th>Update send (secs)</th>
<th>Bloom filter (secs)</th>
<th>Bloom filter (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10K</td>
<td>&lt;1</td>
<td>2</td>
<td>1 M</td>
</tr>
<tr>
<td>1 M</td>
<td>2</td>
<td>24</td>
<td>10 M</td>
</tr>
<tr>
<td>5 M</td>
<td>7</td>
<td>175</td>
<td>50 M</td>
</tr>
</tbody>
</table>
Reliable Wide Area Data Replication

LIGO Gravitational Wave Observatory

Replicating >1 Terabyte/day to 8 sites
>30 million replicas so far
MTBF = 1 month

www.globus.org/solutions
GT4 Execution Management

- Grid Telecontrol Protocol
- Community Scheduling Framework
- Workspace Management
- Grid Resource Allocation & Management
- Pre-WS Grid Resource Alloc. & Mgmt
- Execution Mgmt
Execution Management (GRAM)

- Common WS interface to schedulers
  - Unix, Condor, LSF, PBS, SGE, ...
- More generally: interface for process execution management
  - Lay down execution environment
  - Stage data
  - Monitor & manage lifecycle
  - Kill it, clean up
- A basis for application-driven provisioning
GT4 WS GRAM

- 2nd-generation WS implementation optimized for performance, flexibility, stability, scalability
- Streamlined critical path
  - Use only what you need
- Flexible credential management
  - Credential cache & delegation service
- GridFTP & RFT used for data operations
  - Data staging & streaming output
GT4 WS GRAM Architecture

Service host(s) and compute element(s)

GT4 Java Container

GRAM services

Delegation

Transfer request

RFT File Transfer

Job events

Local job control

Delegate

ops

GRAM adapter

GridFTP

Remote storage element(s)

FTP data

Client

Job functions

Delegate

Compute element

Local scheduler

User job

Seg

FTP control

FTP data

GridFTP

Job events

Local job control

Delegate

ops

GRAM adapter

GridFTP

Remote storage element(s)
GT4 Information Services

- WebMDS
- Trigger
- Index
- Pre-WS Monitoring & Discovery
- Info Services
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
  - (MDS-Archiver: Xpath on historical data)
- Deep integration with Globus containers & services: every GT4 service is discoverable
  - GRAM, RFT, GridFTP, CAS, ...
GT4
Monitoring & Discovery

WS-ServiceGroup
Registration & WSRF/WSN Access

GT4 Container
MDS-Index
adapter

Custom protocols for non-WSRF entities

GT4 Container
MDS-Index
Automated registration in container

GRAM
User

GridFTP

RFT

Clients (e.g., WebMDS)

BRIITE Meeting: The Globus Toolkit
GT4 Documentation is Extensive!
Working with GT4

- Download and use the software, and provide feedback
  - Join gt4friends@globus.org mail list
- Review, critique, add to documentation
- Tell us about your GT4-related tool, service, or application
  - Email info@globus.org
Silver Bullet Hype-Curve...

OGSA: Open Grid Services Architecture
WSRF: WebServices Resource Framework

Globus + OGSA + WSRF + WebServices

Success/Maturity/Acceptance

CORBA

DCE

WebServices

Time

Nov 3, 2005

BRIITE Meeting: The Globus Toolkit
Outline

- Globus Alliance
- Grids
- Globus Toolkit Introduction
- Virtual Organizations
- GT’s BIG Security “Issue”
- Questions & Discussion
Objective: Enable Cross-Organizational Collaboration
Security of Grid Brokering Services

- It is expected brokers will handle resource coordination for users
- Each Organization enforces its own access policy
- User needs to delegate rights to broker which may need to delegate to services
- QoS/QoP Negotiation and multi-level delegation
Security Objective: Forceful Enforcement (?)
Security Services Objectives

- It’s all about “Policy”
  - (Virtual) Organization’s Security Policy
  - Security Services facilitate the enforcement

- Security Policy to facilitate “Business Objectives”
  - Related to higher level “agreement”

- Security Policy often delicate balance
  - More security ⇐ Higher costs
  - Less security ⇐ Higher exposure to loss
  - Risk versus Rewards
  - Legislation sometimes mandates minimum security
Security: Risk versus Reward

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.
Agreement ⇔ VO Security Policy

(Business) Agreement

Price
Cost
Obligations
QoS
T&Cs

Security

Dynamic VO Security Policy

members
resources
roles

Attribute mgmt
Authz mgmt

Static Initial VO Security Policy

trust anchors
(initial) members
(initial) resources
(initial) roles

Access rules
Privacy rules
Virtual Organization (VO) Concept

- VO for each application/workload/collaboration
- Carve out and configure resources for a particular use and set of users
Effective Policy Governing Access Within A Collaboration
Why Grid Security is Hard…(1)

- Resources being used may be valuable & the problems being solved sensitive
  - Both users and resources need policy enforcement
- Dynamic formation and management of Virtual Organizations (VOs)
  - Large, dynamic, unpredictable...
- VO Resources and Users are often located in distinct administrative domains
  - Can’t assume cross-organizational trust agreements
  - Different mechanisms & credentials
    - X.509 vs Kerberos, SSL vs GSSAPI,
    - X.509 vs. X.509 (different domains),
    - X.509 attribute certs vs SAML assertions
Why Grid Security is Hard...(2)

- Interactions are not just client/server, but service-to-service on behalf of the user
  - Requires delegation of rights by user to service
  - Services may be dynamically instantiated
- Standardization of interfaces to allow for discovery, negotiation and use of resources/services
- Implementation must be broadly available & applicable
  - Standard, well-tested, well-understood protocols; integrated with wide variety of tools
- Policy from sites, VO, users need to be combined
  - Varying formats
- Want to hide as much as possible from applications!
The Grid Trust solution

- Instead of setting up trust relationships at the organizational level
  (lots of overhead, possible legalities - expensive!)
  => set up trust at the user/resource level
- Virtual Organizations (VOs) for multi-user collaborations
  - Federate through mutually trusted services
  - Local policy authorities rule
- Users able to set up dynamic trust domains
  - Personal collection of resources working together based on trust of user
Propagation of Requester’s Rights through
Job Scheduling and Submission Process

Virtualization complicates Least Privilege Delegation of Rights.

Dynamically limit the Delegated Rights more as Job specifics become clear.

Trust parties downstream to limit rights for you... or let them come back with job specifics such that you can limit them.
Grid Security must address...

- Trust between resources without organization support
- Bridging differences between mechanisms
  - Authentication, assertions, policy...
- Allow for controlled sharing of resources
  - Delegation from site to VO
- Allow for coordination of shared resources
  - Delegation from VO to users, users to resources
- ...all with dynamic, distributed user communities and least privilege.
Outline

- Globus Alliance
- Grids
- Globus Toolkit Introduction

- Virtual Organizations
- GT’s BIG Security "Issue"

- Questions & Discussion
Security Services with VO
GT’s GGF’s Authorization Call-Out Support

- **GGF’s OGSA-Authz WG:**
  “Use of SAML for OGSA Authorization”
  - Authorization service specification
  - Extends SAML spec for use in WS-Grid
  - Recently standardized by GGF
- **Conformant call-out integrated in GT**
  - Transparently called through configuration
- **Permis interoperability**
  - Ready for GT4!
- **Futures...**
  - SAML2.0 compliance ... XACML2.0-SAML2.0 profile
GT-XACML Integration

- eXtensible Access Control Markup Language (XACML)
  - OASIS standard
  - Open source implementations
- XACML: sophisticated policy language
- Globus Toolkit ships with XACML runtime
  - Integrated in every client and server build on GT
  - Turned-on through configuration

...can be called transparently from runtime and/or explicitly from application...

...and we’re using the XACML-“model” for our Authz Processing Framework...
GT’s Assertion Processing “Problem”

- VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions
- XACML/SAML/CAS/XCAP/Permis/ProxyCert authorization assertions
- Assertions can be pushed by client, pulled from service, or locally available
- Policy decision engines can be local and/or remote
- Delegation of Rights is required “feature” implemented through many different means

GT-runtime has to mix and match all policy information and decisions in a consistent manner...
Delegation of Rights Complexity

Can I have glass of lemonade?
Delegation of Rights Complexity

Ivan’s policy:
I don’t know any Bob…(?)
I do know John, Mary, Carol, Olivia, …

Can I have glass of lemonade?

Bob

Ivan
Delegation of Rights Complexity

Ivan’s policy:
I don’t know any Bob…(?)
I do know John, Mary, Carol, Olivia, …

Can I have glass of lemonade?

Can Bob have glass of lemonade?

Sure, Bob is my friend

Carol’s policy:
Bob is my friend and I’ll share my lemonade with him
Delegation of Rights Complexity

Ivan’s policy:
I don’t know any Bob…(?)
I do know John, Mary, Carol, Olivia, ...

Can I have glass of lemonade?

Can Bob have glass of lemonade?

Mary’s policy:
I like Bob a little bit

Carol’s policy:
If Carol likes Bob, I hate him!

Sure, Bob is my friend

Bob

Ivan

Bob

Carol

Olivia’s policy:
I occasionally like Carol

Lucy’s policy:
I sometimes like Carol

Carol’s policy:
I’ll share my lemonade with him
Delegation of Rights Complexity

Can I have glass of lemonade?

Ivan’s policy:
I don’t know any Bob…(?)
I do know John, Mary, Carol, Olivia, …

Can Bob have glass of lemonade?

Ivan

Carol’s policy:
If Carol likes Bob, I hate him!

Sure, Bob is my friend

Bill’s policy:
Lemonade is bad for you

Can Bob have glass of lemonade?

Bob

Jogger’s policy:
I’d like a glass too

Ivan’s policy:
I don’t know any Bob…(?)
I do know John, Mary, Carol, Olivia, …

Can I have glass of lemonade?

Bill

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?

Ivan

Can I have glass of lemonade?
Delegation of Rights Complexity

Can Bob have a glass of lemonade?

Bob’s policy: I don’t like girls

Bill’s policy: Lemonade is bad for you

Ivan’s policy: I don’t know any Bob… (?)
I do know John, Mary, Carol, Olivia, …

Frosty’s policy: Only share lemonade with ice

Carol’s policy: I sometimes like Carol

I don’t share lemonade with anyone except Ivan

Laura’s policy: Share if he pays!

Ivan’s policy: Sure, Bob is my friend

I’ll share my lemonade with him

Costas’s policy: I like Ivan very much!

I like Ivan very much!

Carol’s policy: If Carol likes Bob, I hate him!

Lucy’s policy: I don’t like girls

I sometimes like Carol

Mary’s policy: I like Bob a little bit

Olivia’s policy: If Carol likes Bob, I hate him!

Jogger’s policy: I’d like a glass too

Laura’s policy: Share if he pays!

Jogger’s policy: I’d like a glass too

Ann’s policy: I like Ivan very much!

Aunt’s policy: Sharing is good

John’s policy: I don’t like girls

Frosty’s policy: Only share lemonade with ice

Can Bob have a glass of lemonade?
Delegation of Rights Complexity

 Neighbor's policy: Let's party!

 Ivan's policy: I don't know any Bob...?!
 I do know John, Mary, Carol, Olivia, ...

 Frosty's policy: Only share lemonade with ice

 Bill's policy: Lemonade is bad for you

 Aunt's policy: Sharing is good

 Carol's policy: If Carol likes Bob, I hate him!

 Laura's policy: Share if he pays!

 Mary's policy: I like Bob a little bit

 Jogger's policy: I'd like a glass too

 Jogger's policy: I'd like a glass too

 Rita's policy: No lemonade after eight

 Emma's policy: Only on his birthday

 Ann's policy: I like Ivan very much!

 John's policy: I don't like girls

 Lucy's policy: I sometimes like Carol

 David's policy: Ask Laura

 Accountant's policy: Only if he signs here

 Sure, Bob is my friend

 Can Bob have a glass of lemonade?

 Sure, Bob is my friend
Delegation of Right Complexity

Neighbor's policy: Let’s party!

Ivan's policy: I don't know any Bob...(?)
I do know John, Mary, Carol, Olivia, …

Can I have a glass of lemonade?

Bill's policy: Lemonade is bad for you

Sure, Bob is my friend

Sure, Bob is my friend and I'll share my lemonade with him

Ivan: HELP
(non-normative evaluated decision)

Laura’s policy: Share if he pays!

Ivan’s policy: I don’t know any Bob...(?)
I do know John, Mary, Carol, Olivia, …

Can I have a glass of lemonade?

Frosty’s policy: Only share lemonade with ice

Jogger's policy: I'd like a glass too

Frosty’s policy: Only share lemonade with ice

Bill’s policy: Lemonade is bad for you

Sure, Bob is my friend and I’ll share my lemonade with him

Carol’s policy: If Carol likes Bob, I hate him!

Lucy’s policy: I sometimes like Carol

Olivia’s policy: If Carol likes Bob, I hate him!

Mary’s policy: I like Bob a little bit

Ann’s policy: I like Ivan very much!

John’s policy: I don’t like girls

Bill’s policy: Lemonade is bad for you

Sure, Bob is my friend

Emma’s policy: Only on his birthday

David’s policy: Ask Laura

Accountant’s policy: Only if he signs here

Laura’s policy: Share if he pays!

Ivan: HELP
(non-normative evaluated decision)
What are the Grid/P2P issues with "distributed authorization"? (1)

- Many different parties want to express their opinion about each other’s access rights
  - Anybody can say anything about anyone else
- Expressed in many different languages
  - Enforcement of single policy language impossible/not-desirable
- Some parties can be asked about their opinion
  - Expose themselves as an AuthZ-oracle (PDP)
- Other parties send their opinion as statements
  - Authenticated policy/decision statements/assertions expressed in their favorite language
What are the Grid/P2P issues with “distributed authorization”? (2)

- Some of that advise is from parties you’ve never met before
  - So they must be empowered by those you do know...
- Some advise does not apply, is mal-formed, malicious, fake, erroneous, ....
  - ...often you do not know that by looking at them...
- Different parties will use different names for the same subject
  - Need identity federation for mapping
- Different parties will use different groups/roles in their policy expressions
  - Only the group/role that is actually used in a relevant policy expression is of interest...
Attribute Collection Framework
GT’s Authorization Processing Model (1)

- Use of a Policy Decision Point (PDP) abstraction that conceptually resembles the one defined for XACML.
  - Normalized request context and decision format
  - Modeled PDP as black box authorization decision oracle
- After validation, map all attribute assertions to XACML Request Context Attribute format
- Create mechanism-specific PDP instances for each authorization assertion and call-out service
- The end result is a set of PDP instances where the different mechanisms are abstracted behind the common PDP interface.
GT’s Authorization Processing Model (2)

- The Master-PDP orchestrates the querying of each applicable PDP instance for authorization decisions.
- Pre-defined combination rules determine how the different results from the PDP instances are to be combined to yield a single decision.
- The Master-PDP is to find delegation decision chains by asking the individual PDP instances whether the issuer has delegated administrative rights to other subjects.
- The Master-PDP can determine authorization decisions based on delegated rights without explicit support from the native policy language evaluators.
GT Authorization Framework (1)
GT Authorization Framework (2)

AAA/PERMIS/XACML

PDP

AAA token

Request

saml authz assertion issued by AaId-2

xacml policy assertion issued by AaId-1

stub-runtime

Policy Decision Point

AuthzSvc config EPR + AaId-3

Service Provider

resource owner (RsrId)

AAA PDP

EPR PDP

local PDP

AuthzSvc EPR

local policy DB

xicml PDP
GT Authorization Framework (3)

● Master-PDP accessed all mechanism-specific PDPs through same Authz Query Interface
  ◆ SAML-XACML-2 profile

● Master PDP acts like XACML “Combinator”
  ◆ “Permit- Overrides” rules
    ● Negative permissions are evil...

● Delegation-chains found through exhaustive search
  ◆ ...with optimization to evaluate cheap decisions first...

● “Blacklist-PDPs” are consulted separately
  ◆ Statically configured, call-out only PDPs
  ◆ Deny- Overrides only for the blacklist-PDPs...
    ● Pragmatic compromise to keep admin simple
Big Picture & Conclusion

- GT4 is security buzzword compliant!
  - ...probably the most full-featured-security ws-toolkit...
- WebServices technologies provide low-level plumbing
  - following all relevant standards
- Portals growing as a user interface
  - Clients use http-browsers,
    ... but portals will use WS-protocols!
  - PURSE, ESG, GridSite, LEAD Portal, ...
- New Deployment Paradigms (GridLogon, VMs)
  - Driven by inability to protect...
- Authorization still the big focus
  - “unification framework” needed to support different mechanisms and formats => GT4.2
  - Required for fine-grained VO-policy
