the globus alliance
www.globus.org

Grid Security: The Globus Perspective

GlobusWORLD 2005

Feb 7-11, Boston, MA

Frank Siebenlist - ANL (franks@mcs.anl.gov)

Von Welch - NCSA (welch@ncsa.uiuc.edu)

http://www.globus.org/

Outline

- Part One: Von Welch, NCSA
- The Big Picture
- What is Grid Security?
- Current Grid Security

- Part Two: Frank Siebenlist, ANL
- 2004: The year we lost control of the desktop
- Leverage Security Service Implementations
- GT's Authorization Processing Framework

- Futures and Conclusion

Big Picture

- X.509 Proxy and End Entity Certificates still backbone of authentication and delegation
  - Proxy Certificates now IETF standard (RFC 3820)
- Web Services technologies are providing more of the low-level plumbing
  - WS-Security
- Portals growing as a user interface
  - Users want "light-weight" interface to Grid
- Authorization still the big focus

What is Grid Security?

The Grid problem is to enable "coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."

From **The Anatomy of the Grid**

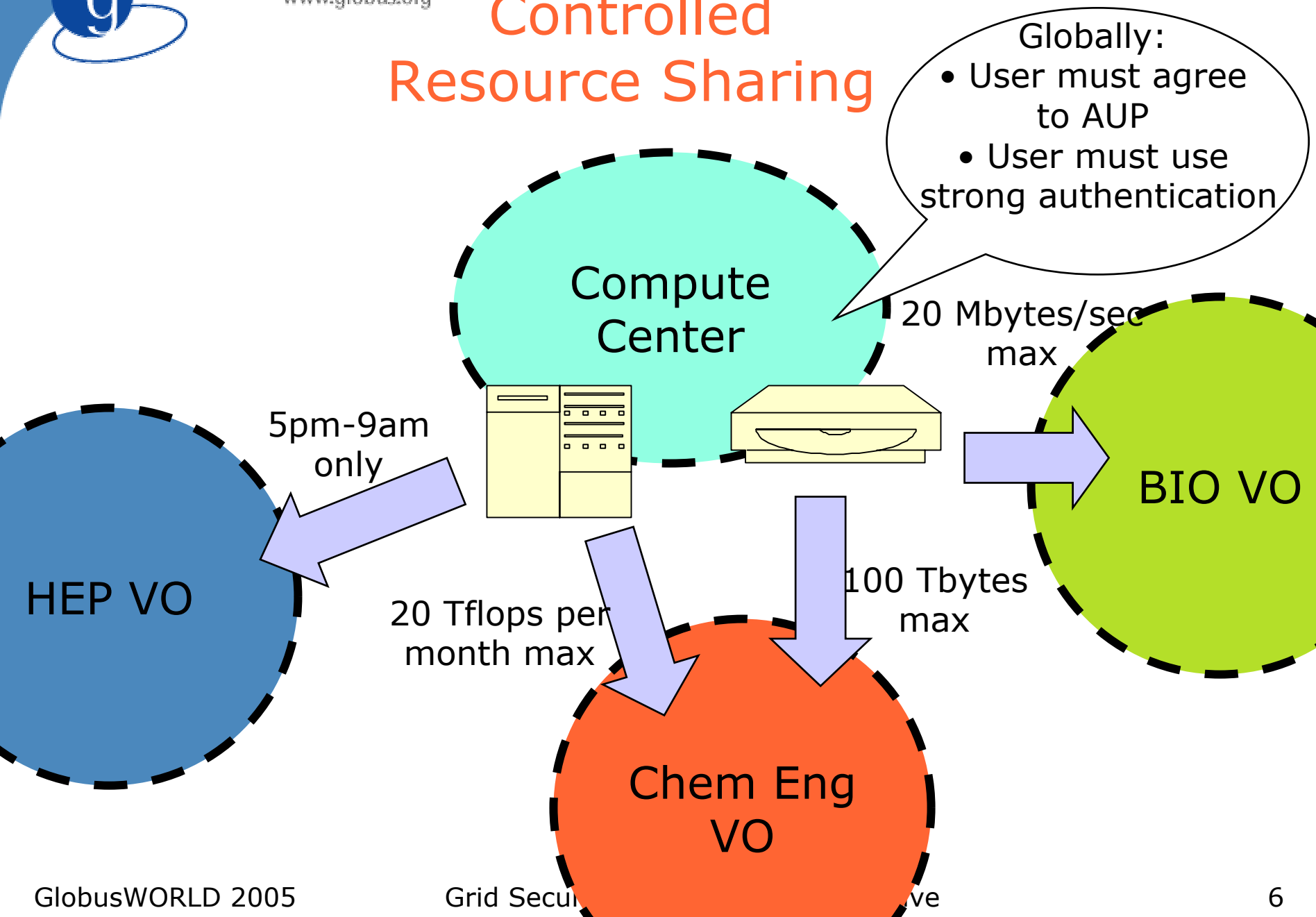
- So Grid Security is security to enable VOs
- What is needed in terms of security for a VO?

Resource Sharing

"…coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."

- Resources being used are still owned by their respective organization and subject to its policies
  - Sharing may be controlled amongst a number of VOs
  - Non-trivial policy in regards to QoS, QoP, etc.

Controlled Resource Sharing



Requires Coordination by VO

"...coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."

- Resources contributed to VO need to be coordinated by the VO in order to work together effectively.
  - All need to have a coherent policy in order to interoperate
  - Requires policy from VO back to resources

Dynamic Users, Resources, Policies

"…coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."

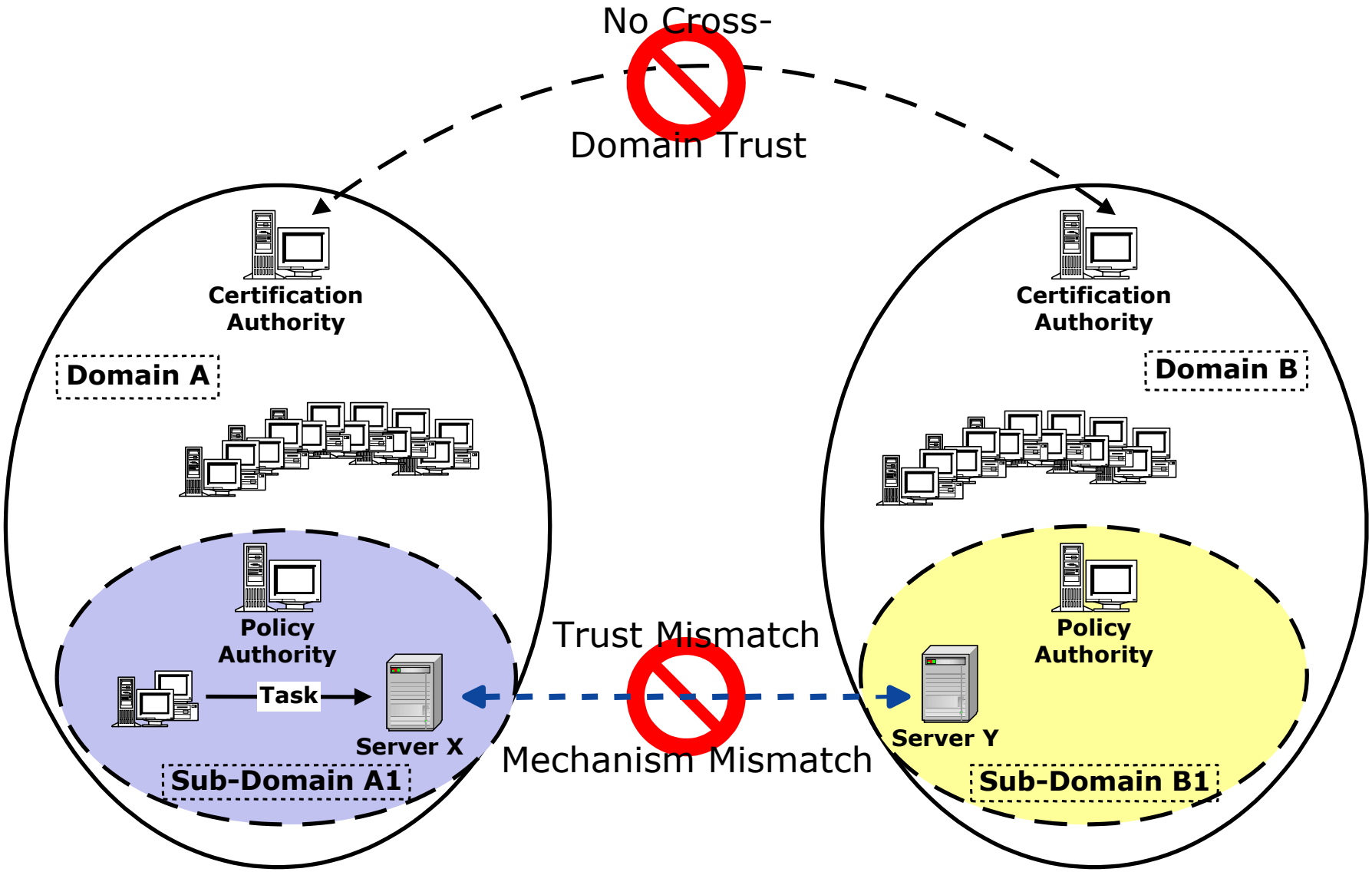
- Users, resources may be large, unpredictable, and changing at any point
- Roles of both may also be distinct and dynamic (not all users are equal).
- Doesn't allow for static configuration

Multiple Organizations, Mechanisms, Policies

"…coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."

- Each resource and user will have local policies and technologies that cannot be replaced by the VO
- Cannot assume cross-organizational trust relationships

Multi-Institution Issues



Why Grid Security is Hard

- Resources being used may be valuable & the problems being solved sensitive
  - Both users and resources need to be careful
- 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

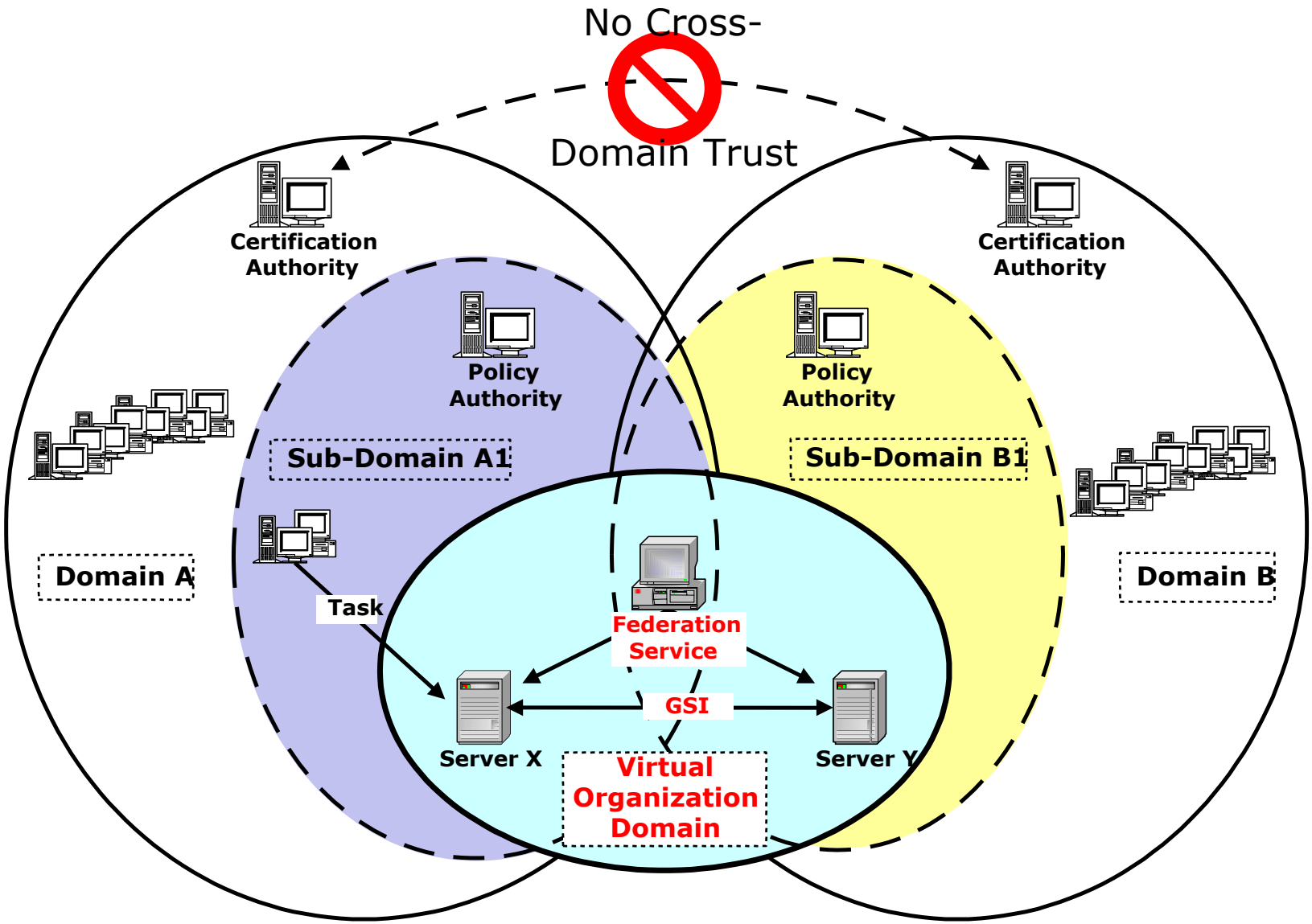
Why Grid Security is Hard…

- 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
- 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!

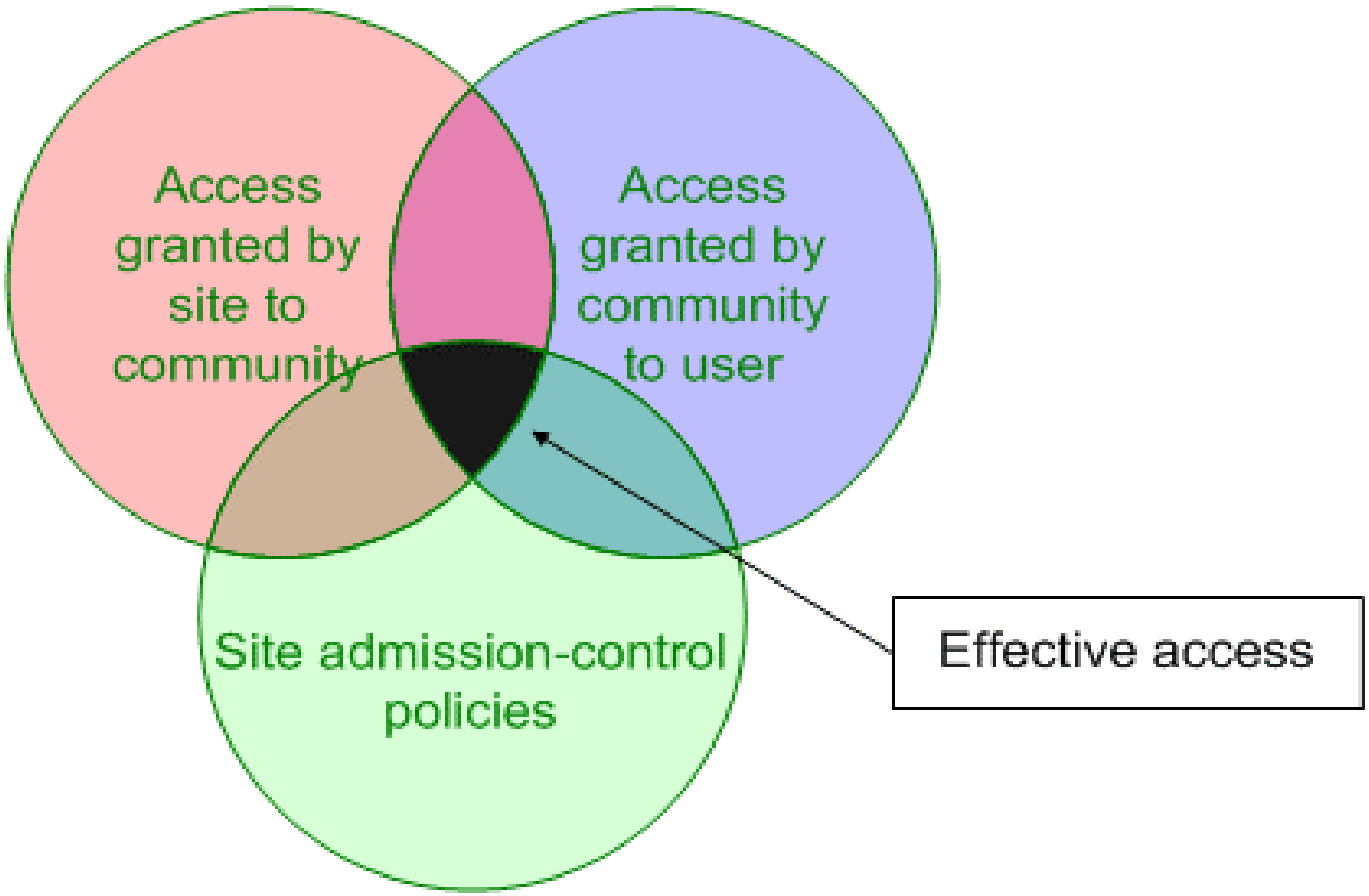
The Grid Trust solution

- 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

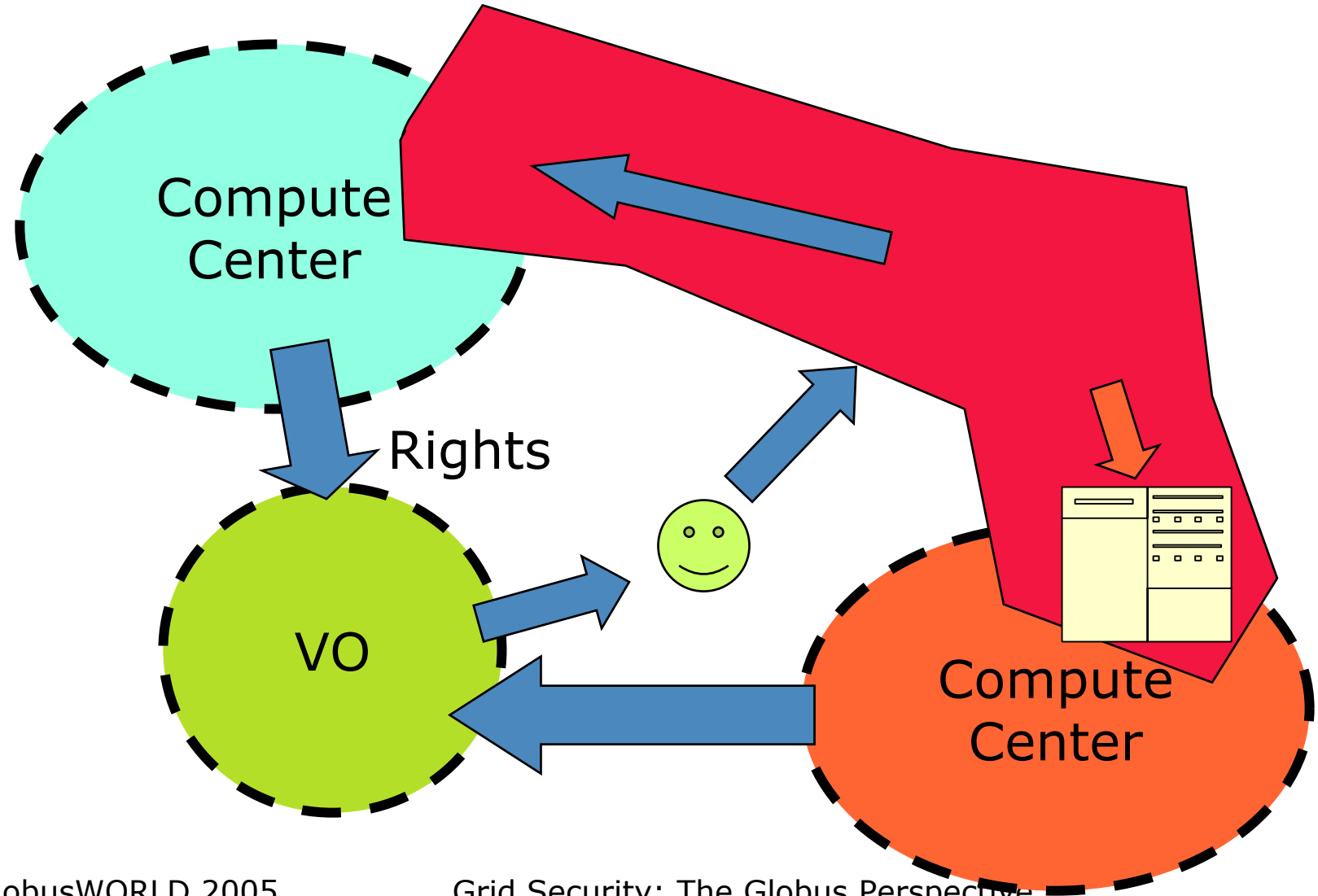
Grid Solution: Use Virtual Organization as Bridge



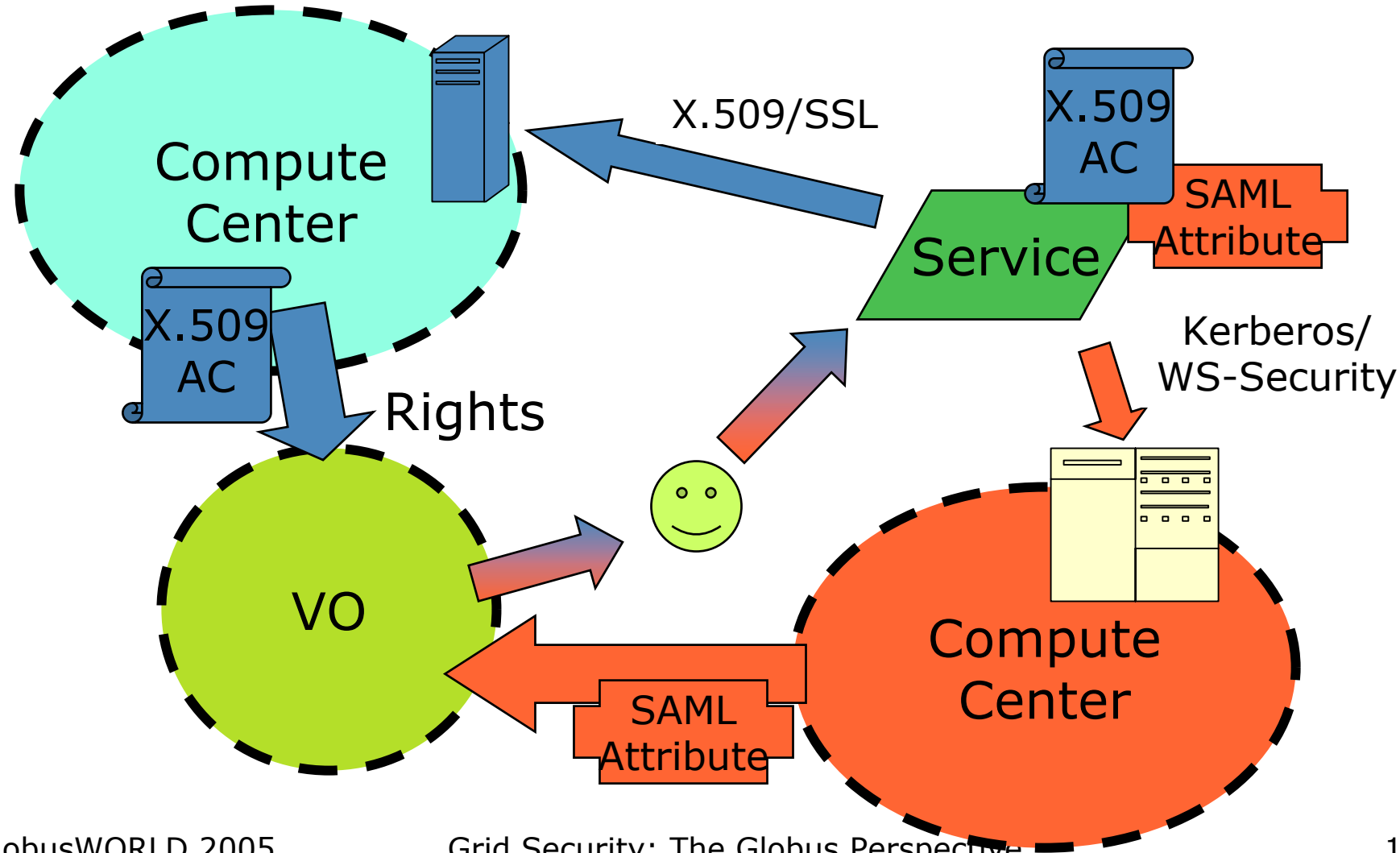
Effective Policy Governing Access Within A Collaboration



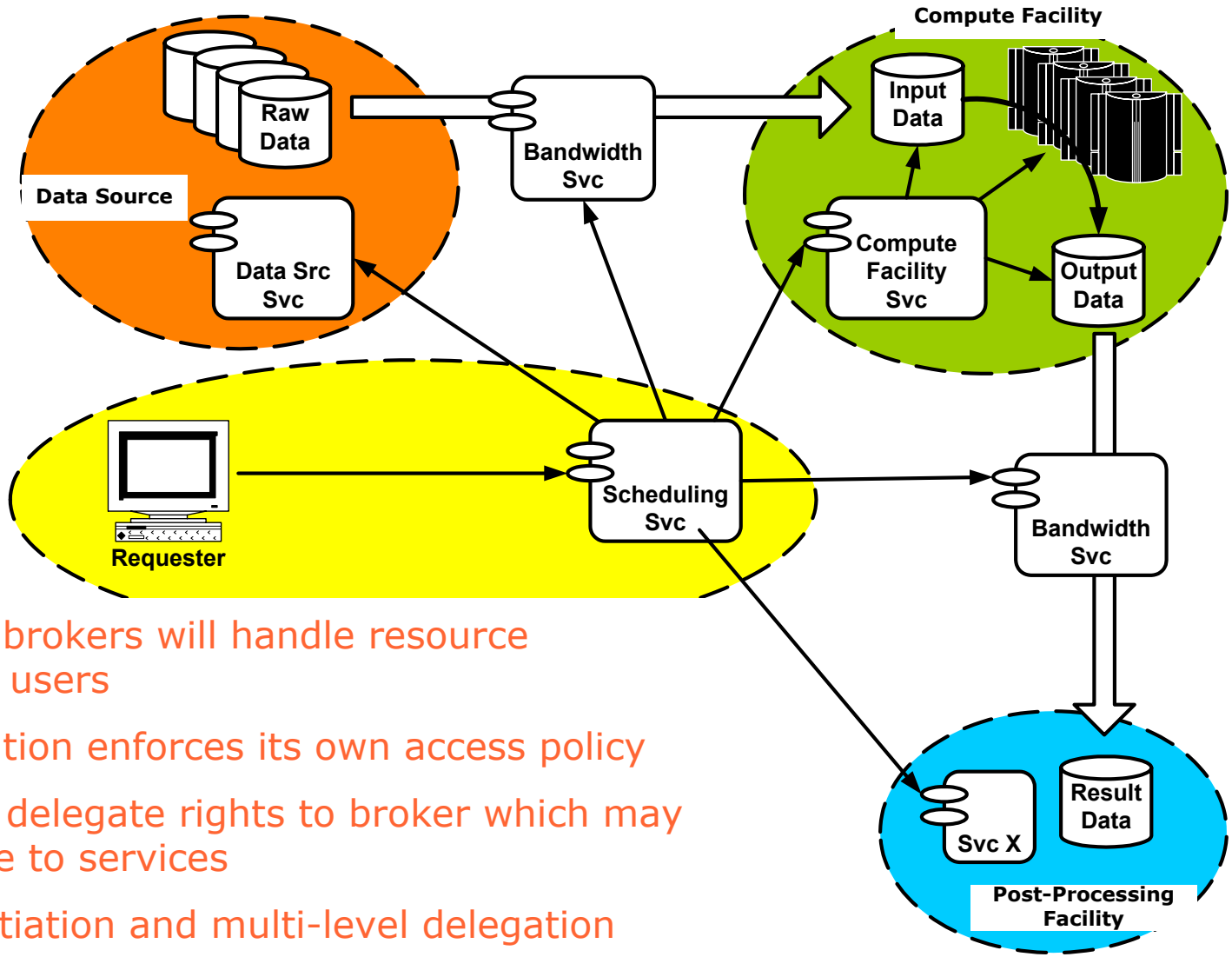
Use Delegation to Establish Dynamic Distributed System



Goal is to do this with arbitrary mechanisms

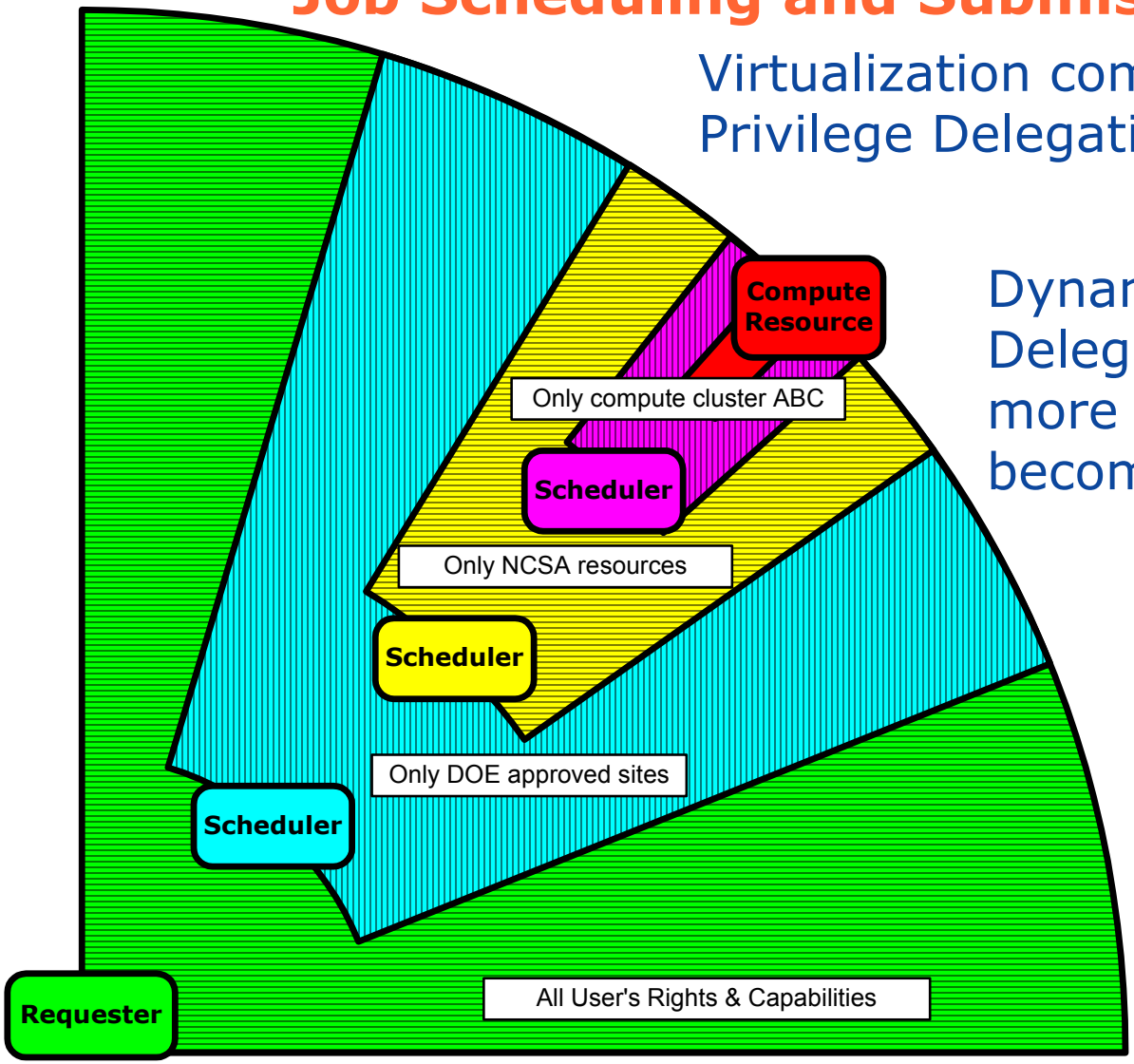


Security of Grid Brokering Services



- 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

Propagation of Requester's Rights through Job Scheduling and Submission Process



Virtualization complicates Least Privilege Delegation of Rights

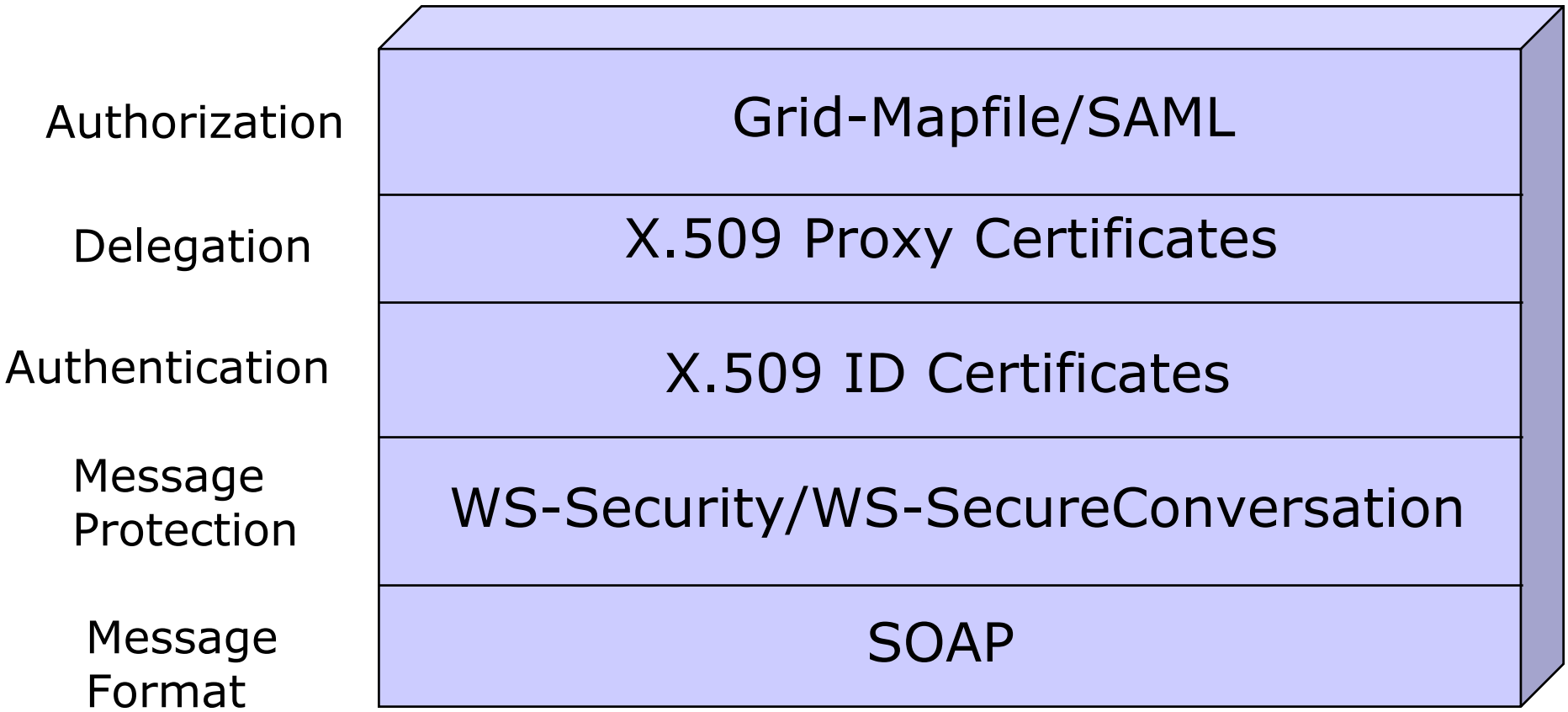
Dynamically limit the Delegated Rights more as Job specifics become clear

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.

Security Layers



Grid Security Infrastructure (GSI)

- Use GSI as a standard mechanism for bridging disparate security mechanisms
  - Doesn't solve trust problem, but now things talk same protocol and understand each other's identity credentials
  - Basic support for delegation, policy distribution
- Translate from other mechanisms to/from GSI as needed
- Convert from GSI identity to local identity for authorization

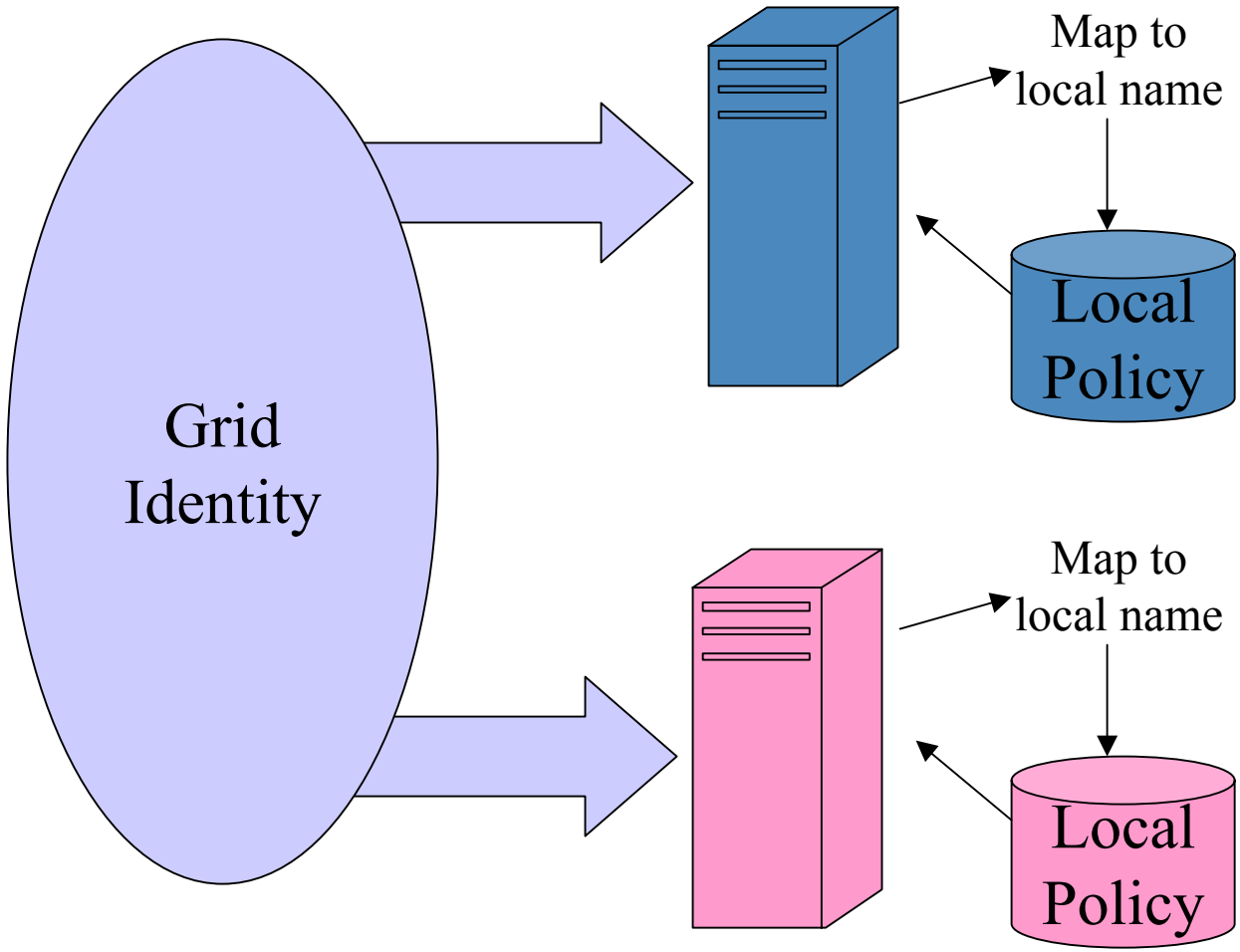
Grid Security Infrastructure (GSI)

- Based on standard PKI technologies
  - CAs allow one-way, light-weight trust relationships (not just site-to-site)
- SSL protocol or WS-Security for authentication, message protection
- X.509 Certificates for asserting identity
  - for users, services, hosts, etc.
- Proxy Certificates
  - GSI extension to X.509 certificates for delegation, single sign-on

Grid Identity, Local Policy

- In current model, all Grid entities assigned a PKI identity.
- User is mapped to local identities to determine local policy.

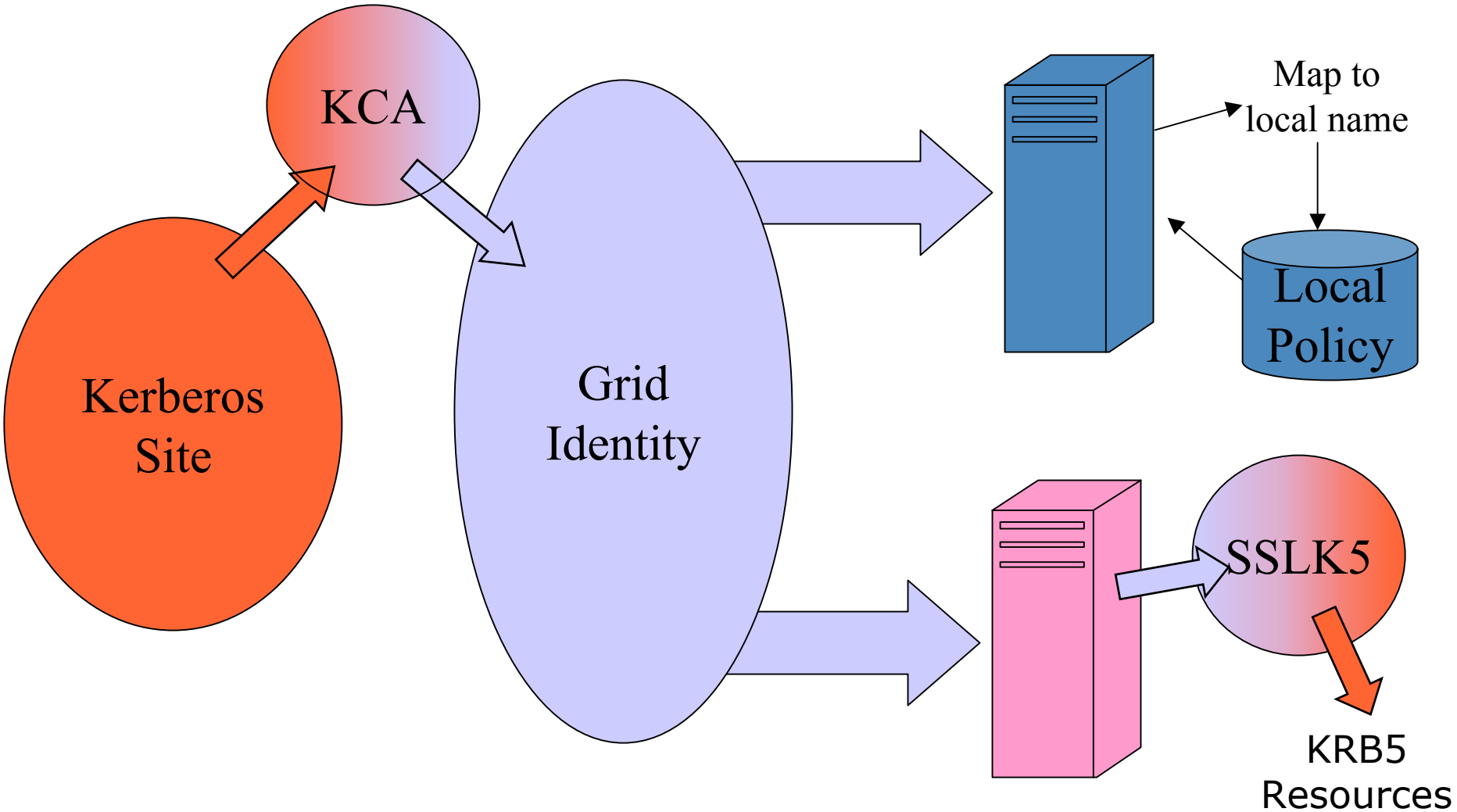
.



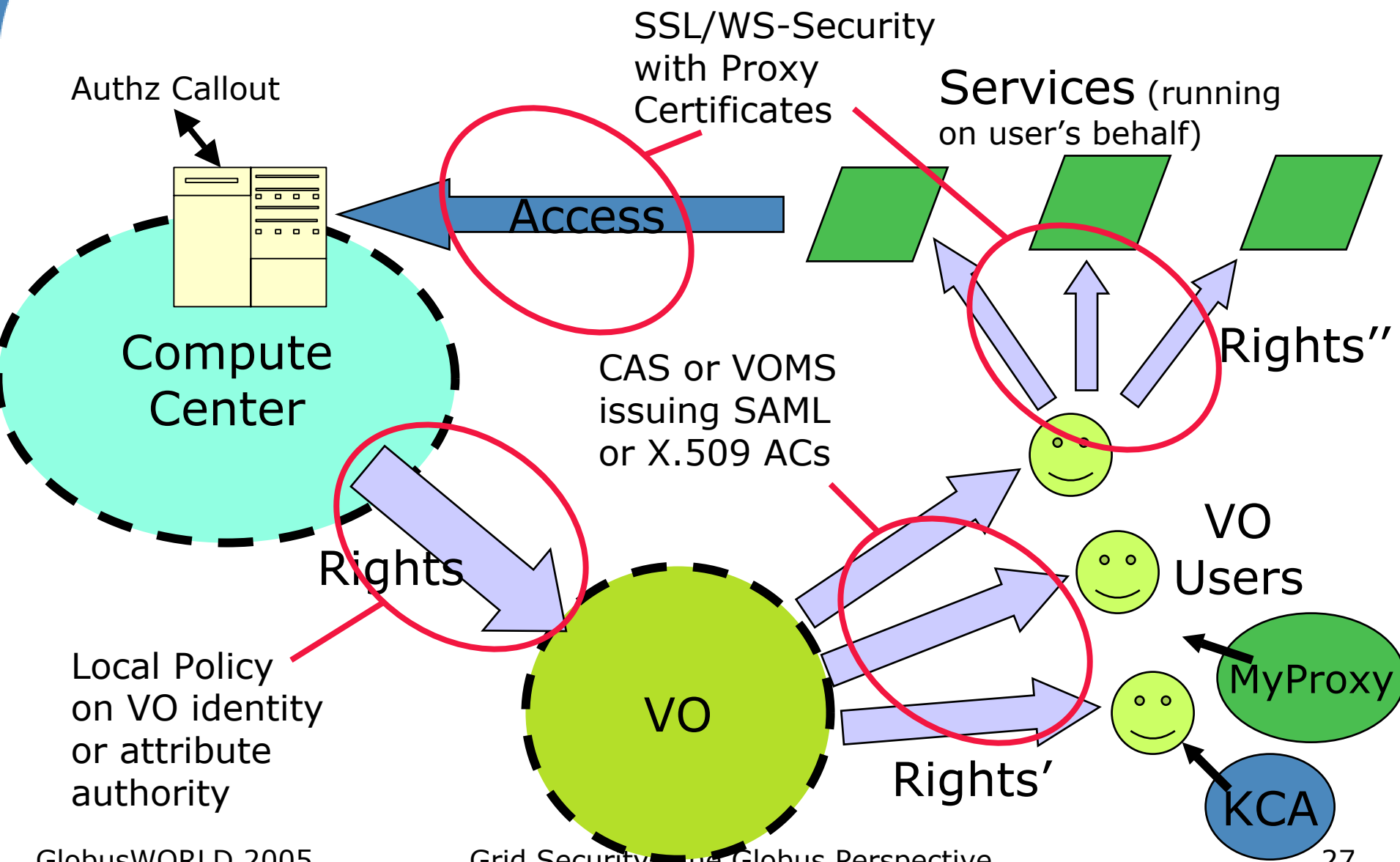
Kerberos to GSI Gateway

- To use Kerberos, a Kerberos-to-GSI gateway translates Kerberos credentials to GSI credentials to allow local Kerberos users to authenticate on the Grid.
  - Kx509/KCA is an implementation of one such gateway.
- Sslk5/pkinit provide the opposite functionality to gateway incoming Grid credentials to local Kerberos credentials.

Local Identity, Grid Identity, Local Policy



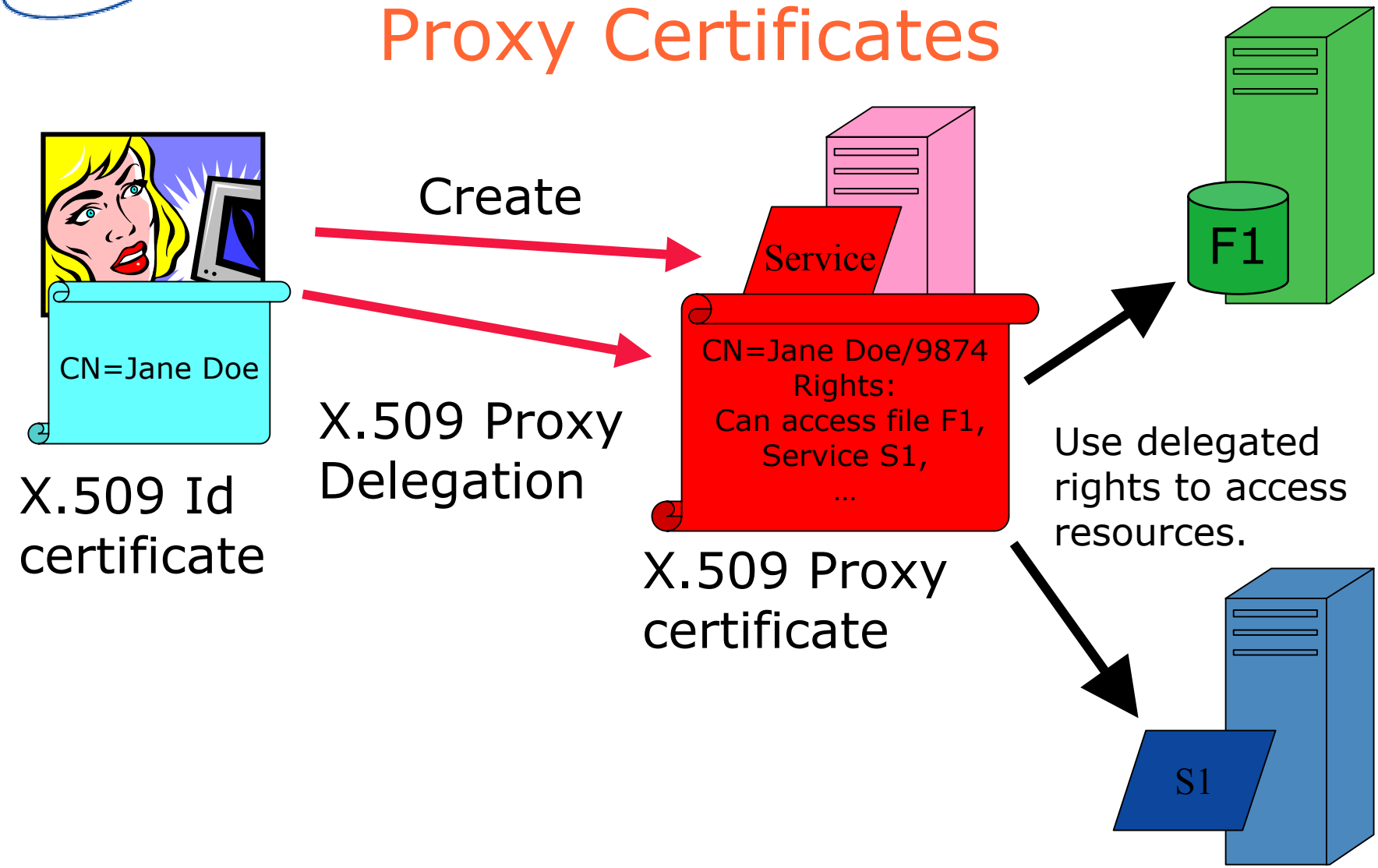
GSI Implementation



X.509 Proxy Certificates

- GSI Extension to X.509 Identity Certificates
  - RFC 3820
  - Support being added to OpenSSL
- Enables single sign-on
- Allow user to dynamically assign identity and rights to service
  - Can name services created on the fly and give them rights (i.e. set policy)
- What is effectively happening is the user is creating their own trust domain of services
  - Services trust each other with user acting as the trust root

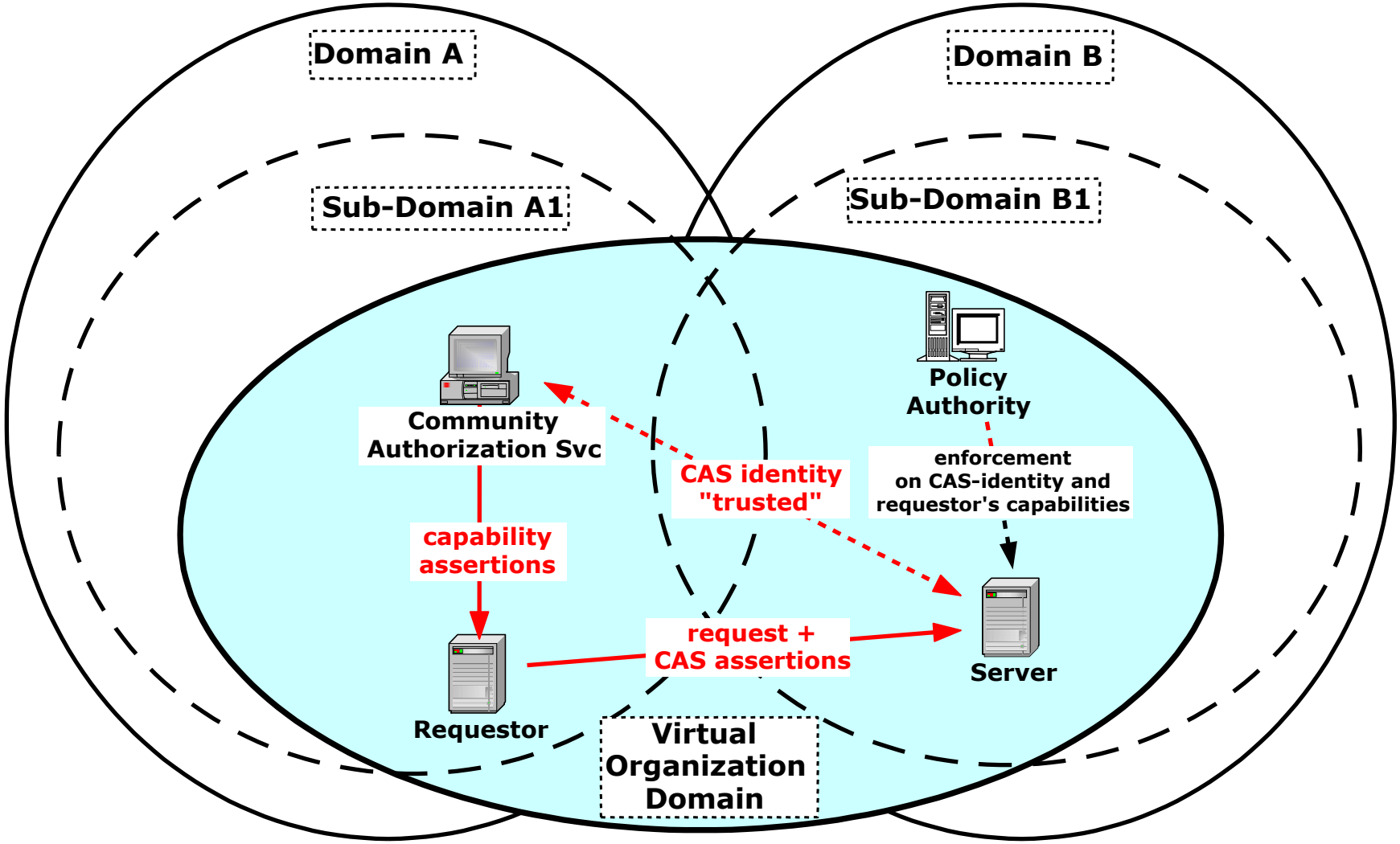
Proxy Certificates



Community Authorization Service

- Question: How does a large community grant its users access to a large set of resources?
- Community Authorization Service (CAS)
  - Outsource policy admin to VO sub-domain
  - Enables fine-grained policy
- Resource owner sets 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 that get enforced at the resource

Community Authorization Service



MyProxy: Credential Wallet/Converter

- MyProxy allows users to store GSI credentials and retrieve them
  - With username/pass phrase or other credential
  - Can act as a credential translator from username/passphrase to GSI
- Used by services that can only handle username and pass phrases to authenticate to Grid
  - Services limited by client implementations
    - E.g. web portals
- Also handle credential renewal for long-running tasks

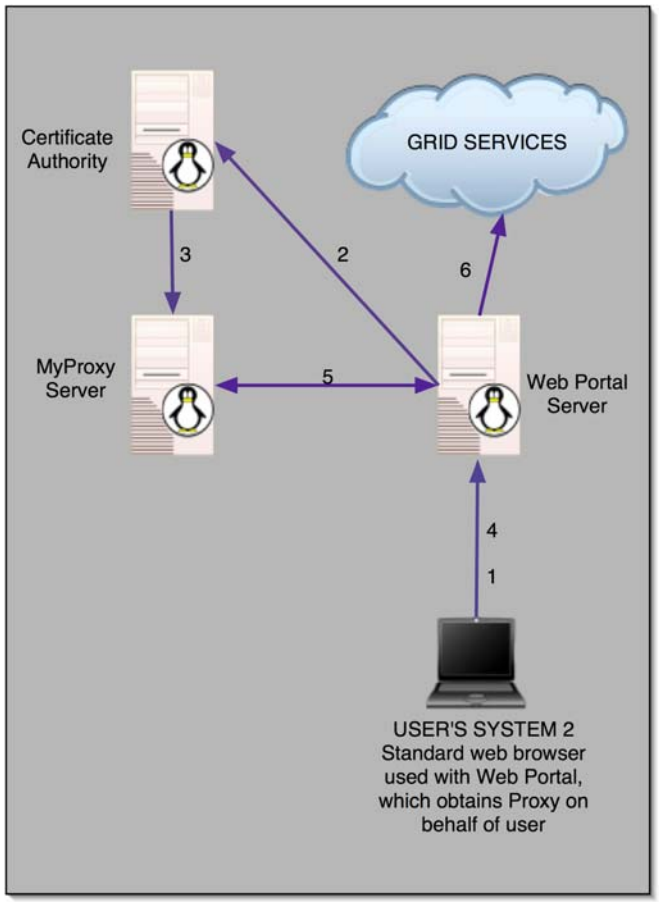
MyProxy - One-Time-Password

- MyProxy now supports SASL and PAM for authentication
- PAM plugins for one-time passwords (OTP) allow for bridging between OTP and Grid security
  - User authenticates to MyProxy via OTP and gets short-term Grid credential in return

Beyond Local Identity for Authorization

- Mapping to local identity works ok, but has limitations
  - Scalability, granularity, consistency…
- Requirement for greater flexibility
- Pre-WS GRAM, GridFTPd have simple API callout to deployment-time libraries/services
- GT4 Web Services-based implement:
  - Standardized version based on GGF/OASIS SAML work
  - Axis Handlers to implement custom authorization schemes

Portal-based Grid Interface: PURSE



- Portal extensions (CGI scripts) that automate user registration requests.
  - Solicits basic data from user.
  - Generates cert request from CA (implemented with "simple CA" from GT).
  - Admin interface allows CA admin to accept/reject request.
  - Generates a certificate and stores in MyProxy service.
  - Gives user ID/password for MyProxy.
- Benefits
  - Users never have to deal with certificates.
  - Portal can get user cert from MyProxy when needed.
  - Database is populated with user data.
- This can be reused in other projects!

Delegation Service

- Exposes delegated credentials as first class resource
- Allows for resource across multiple services
  - E.g. multiple jobs, RFT requests
- Allows for explicit destruction and renewal

Part 2 Outline (Frank)

- **2004: The year we lost control of the desktop**
  - **MyProxy/GridLogon, OTP/Smart-Cards, Secure-Password Protocols, Virtual Machines,…**
- Leverage Security Service Implementations
  - OpenSSL, OpenSAML, Shibboleth, Permis, Sun's XACML, CNRI's Handle System, … XKMS
- GT's Authorization Processing Framework
  - VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions
  - XACML/SAML/CAS/Permis/ProxyCert/SPKI authorization assertions
- Futures and Conclusion

2004: The Year we lost Control of the Desktop

- Compromised accounts, trojans, sniffers, viruses…
  - **When** compromised … not if…
- New paradigm:
  - Try to raise bar … arms race
  - It's about "Detection" and "Limit Consequences" of Compromise
- New emphasis:
  - No more long-lived secrets with the user…
  - MyProxy/GridLogon
  - One-Time-Password & Secure Password protocols
  - Virtual Machine Sandboxes

MyProxy/GridLogon

- No long-lived secrets on the user's workstation
  => move secrets to a secure MyProxy-server
  - Issue derived short-lived proxy-certificates

  => issue short-lived identity certificates
  - On-line Certificate Authority (CA)
- Need for bootstrap authentication…
  - Passwords
  - One-Time-Passwords
- Need for "true" secure password protocol
  - See "Secure (One-Time-) Password Authentication for the Globus Toolkit"
- GW05: "Using the MyProxy Online Credential Repository"
  - Jim Basney (NCSA)
  - Wed Feb 9, 10:30am, Session 4b, Back Bay A

OTP & Secure Password Protocol

- One-Time-Password "issues"
  - Exchange in the clear - hijacking risk
  - No mutual authentication
- Password authentication "issues"
  - Off-line dictionary attacks
  - Clear-text over SSL relies on server trust root on (untrusted) client
- Need for "true" secure password protocol
  - Integrate OTP
- GW05: "Secure (One-Time-) Password Authentication for the Globus Toolkit"
  - Olivier Chevassut (Lawrence Berkeley National Lab.)
  - Thu, Feb 10, 10:30am, Session 7b, Back Bay A

Virtual Machines to the Rescue

- VM's provide additional insulation
  - Consequences of VM compromise "limited"
  - Host compromise "virtually" impossible
- "Frozen" VM-Image of stable, tested, uncompromised OS+Services configuration
  - Distribution of "safe" VM-images
  - Allows for easy restart/resync after compromise
- Interesting open source VM-efforts: Xen
  - Exciting&promising first results at ANL (Tim Freeman, Kate Keahey)
- GW05: "Virtual Machines as Virtual Resources in the Grid"
  - Kate Keahey (ANL)
  - Thu, Feb 10, 10:30am, Session 7b, Back Bay A

Part 2 Outline (Frank)

- 2004: The year we lost control of the desktop
  - MyProxy/GridLogon, OTP/Smart-Cards, Secure-Password Protocols, Virtual Machines,…
- **Leverage Security Service Implementations**
  - **OpenSSL, OpenSAML, Shibboleth, Sun's XACML, Handle System, … Permis, XKMS**
- GT's Authorization Processing Framework
  - VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions
  - XACML/SAML/CAS/Permis/ProxyCert/SPKI authorization assertions
- Futures and Conclusion

Leverage (Open Source) Security Service Implementations

- OpenSSL
  - "native" Proxy Certificate support coming…
    (**thanks to OpenSSL hacker Richard Levitte and KTH!**)
- Internet2's OpenSAML
  - Part of GT - used by CAS/GridShib/AuthzCallout/…
- Internet2's Shibboleth
  - NSF funded GridShib project to "Grid-enable" Shibboleth
- Sun's open source XACML effort
  - Integrate sophisticated policy decision engine in the GT
- CNRI's Handle System
  - Leverage robust, secure, global naming system for resource/subject attribute bindings
- Futures: XKMS, XrML, Permis, …

GT - Shibboleth Integration

- NSF-funded "GridShib" Project
  - http://grid.ncsa.uiuc.edu/GridShib/
- Leverage Shibboleth implementations and deployments
  - Sophisticated, policy controlled attribute service
  - Client-server interactions through WS-protocols
  - (optionally) preserve pseudonymity of client
- GridShib code will become part of GT
  - Transparent use of Shib servers in GT-runtime
- GW05:" Grid-Shibboleth Integration: A Policy Controlled Attribute Framework"
  - Tom Barton (UofChicago), Kate Keahey (ANL), Frank Siebenlist (ANL), Von Welch(NCSA)
  - Tue Feb 8, 10:30am, Session 1b, Back Bay A

Earth System Grid's use of CAS plumbing

- Globus' Community Authorization System (CAS)
  - Uses SAML Authorization Decision Assertions (based on OpenSAML)
- Earth System Grid (ESG) Portal Application
  - Own dedicated authorization system
  - Generates CAS-compliant Authz Assertions
  - Reuse of the CAS-enabled GridFtp services
- Usage Pattern applicable to many more projects…
- GW05: "(Reusable) Portal-based Authorization Solution for the Earth System Grid SciDAC Project"
  - Veronika Nefedova (ANL)
  - Wed Feb 9, 10:30am, Session 4b, Back Bay A

GT-XACML Integration

- eXtensible Access Control Markup Language (XACML)
  - OASIS standard
  - Open source implementations
- XACML: sophisticated policy language
- Globus Toolkit will ship with XACML runtime
  - Integrated in every client and server build on GT
  - Working on integration details right now…
- GW05: "Access Control for the Grid"
  - Anne Anderson (Sun - OASIS/XACML TC)
  - Takuya Mori (NEC - visiting researcher at ANL)
  - Tue Feb 8, 10:30am, Session 1b, Back Bay A
- Demo: GT-XACML Integration plus Delegation of Rights
  - Takuya Mori in CyberCafe

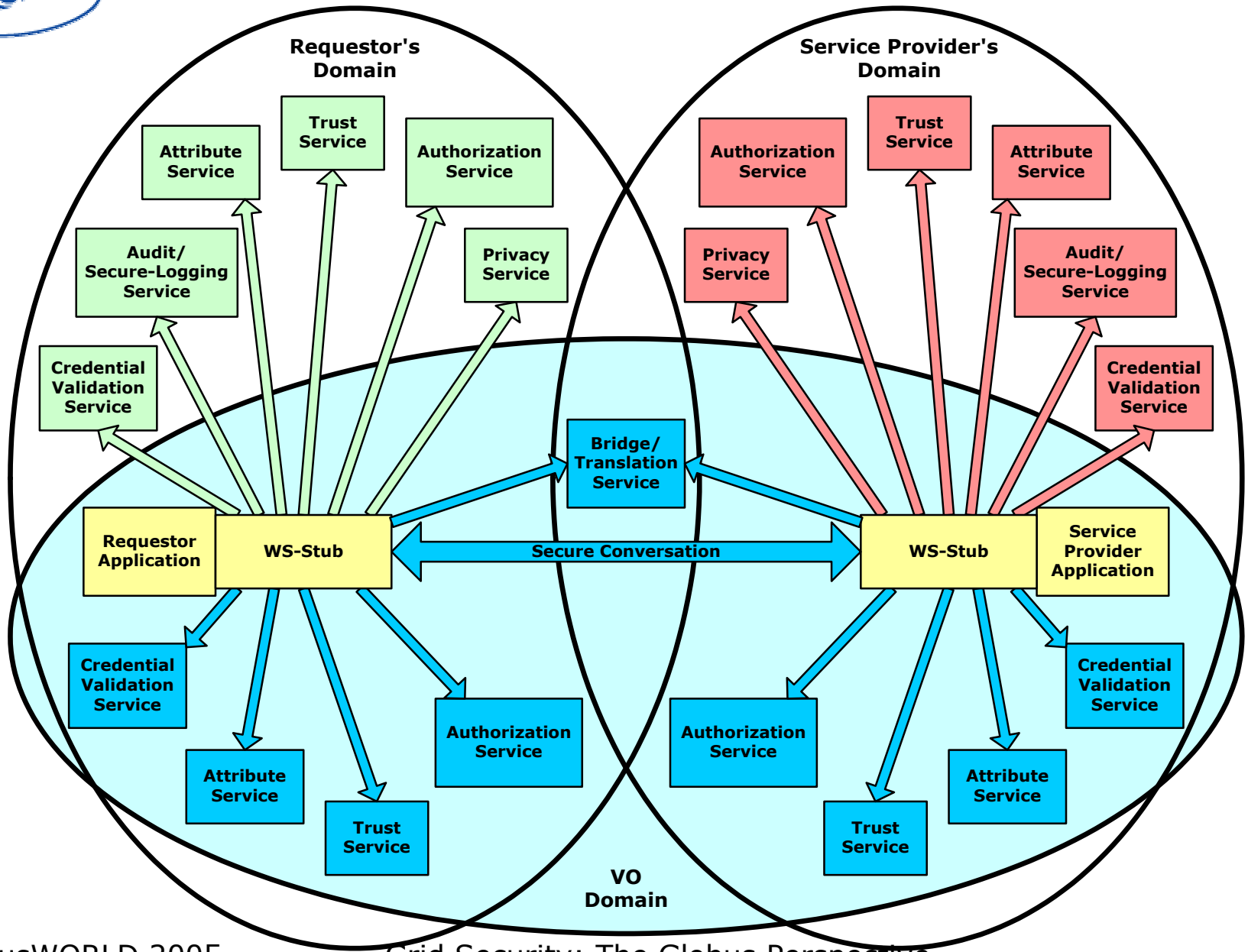
GT - Handle-System Integration

- Corporation for National Research Initiatives' Handle System:
  - Secure, scalable, global naming system (…DNS on steroids)
- Open Source client/server implementations with CNRI deploying global root services
  - Allows for global name resolution
- Many uses for Handles/Digital-Objects
  - Directory/naming service for all kinds of attribute bindings
  - Location service for ResourceId-EPR resolution
- Handle Server implementation backend for …
  - SAML/XKMS/Resource-Properties services
- GW05: "The Globus Toolkit and the Handle System: A Powerful Combination"
  - Sam X. Sun (CNRI)
  - Wed Feb 9, 1:30pm, Session 5b, Back Bay A
- "Walking Counter" Demo of GT-HandleSystem Integration
  - Sam Sun @ CyberCafe

Part 2 Outline (Frank)

- 2004: The year we lost control of the desktop
  - MyProxy/GridLogon, OTP/Smart-Cards, Secure-Password Protocols, Virtual Machines,…
- Leverage Security Service Implementations
  - OpenSSL, OpenSAML, Shibboleth, Permis, Sun's XACML, CNRI's Handle System, … XKMS
- **GT's Authorization Processing Framework**
  - **VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions**
  - **XACML/SAML/CAS/Permis/ProxyCert/SPKI authorization assertions**
- Futures and Conclusion

OGSA Security Services



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
  - XACML coming…
- Futures…
  - SAML2.0 compliance … XACML2.0-SAML2.0 profile

GT's Assertion Processing "Problem"

- VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions
- XACML/SAML/CAS/XCAP/Permis/ProxyCert/SPKI 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…

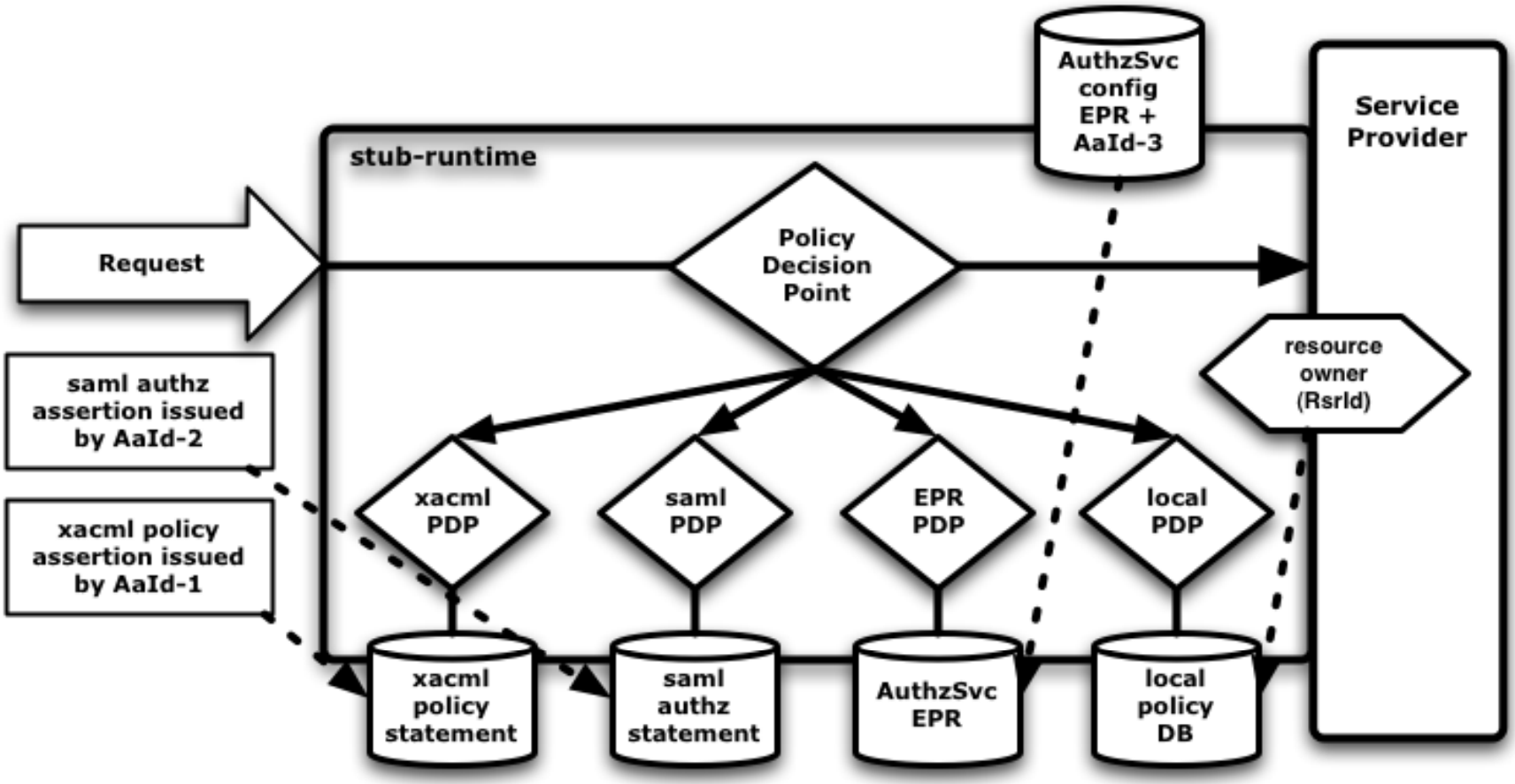
GT's Authorization Processing Model

- 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.

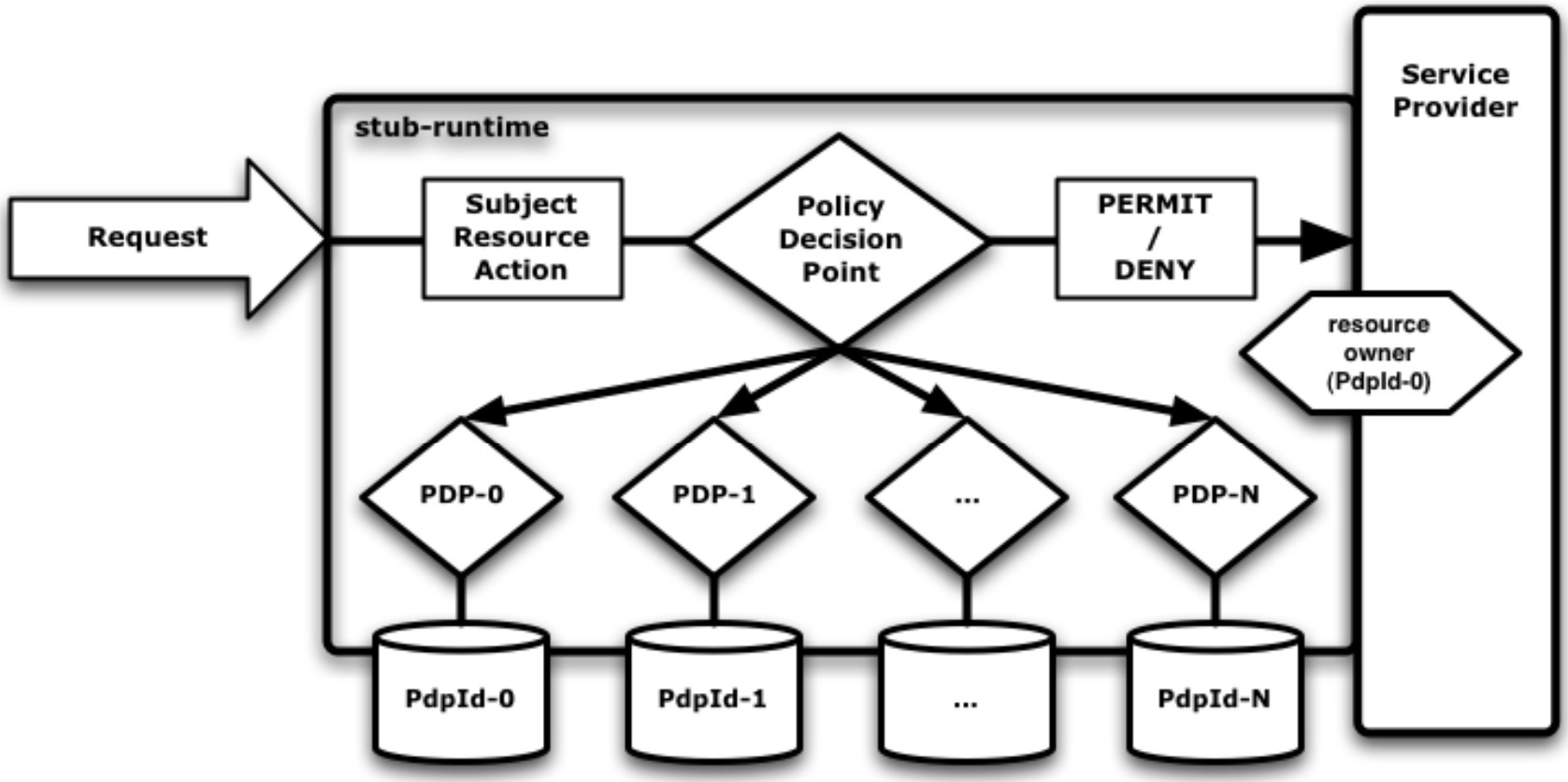
GT's Authorization Processing Model (2)

- 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)



GT Authorization Framework (3)

- Work in progress…
  - Not part of GT4.0
- Note that we "have" to solve this problem…
- Demo in CyberCafe
  - Takuya Mori (NEC/ANL)

Part 2 Outline (Frank)

- 2004: The year we lost control of the desktop
  - MyProxy/GridLogon, OTP/Smart-Cards, Secure-Password Protocols, Virtual Machines,…
- Leverage Security Service Implementations
  - OpenSSL, OpenSAML, Shibboleth, Permis, Sun's XACML, CNRI's Handle System, … XKMS
- GT's Authorization Processing Framework
  - VOMS/Permis/X509/Shibboleth/SAML/Kerberos identity/attribute assertions
  - XACML/SAML/CAS/Permis/ProxyCert/SPKI authorization assertions
- **Futures and Conclusion**

Big Picture & Futures

- X.509 Proxy and End Entity Certificates still backbone of authentication and delegation
  - …but support for more expressive assertion languages (SAML/XACML) will allow alternatives…
- Web Services technologies are providing more of the low-level plumbing
  - Use of SOAP-Header instead of ProxyCert embedding for communication of security info
- Portals growing as a user interface
  - Clients use http, … but portals will use WS-protocols!
- Authorization still the big focus
  - "unification framework" needed to support different mechanisms and formats

Conclusion

- **Great progress in GT's Security Functionality**
- **Great achievements by Globus' Coders!**
- **Great leverage of "external" efforts**
- **Great amount of work still to be done…**
- **Great need for more support and collaboration**