Grid Security: The Globus Perspective

Steve Tuecke

April 7, 2004

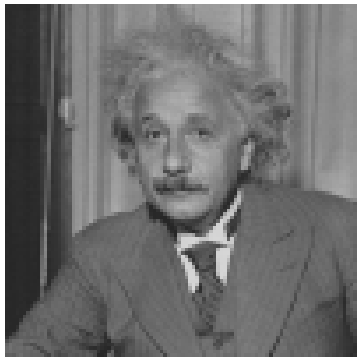
http://www.globus.org/

the globus alliance
www.globus.org

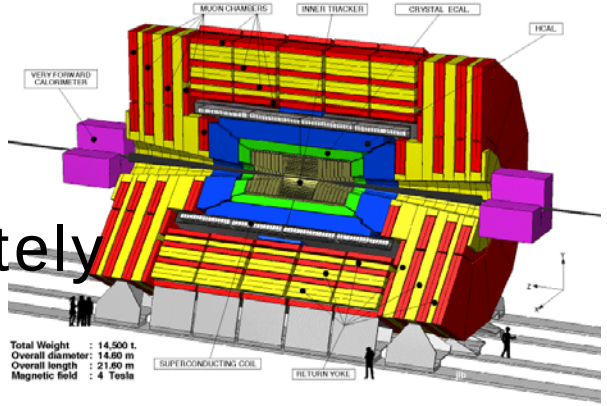
Outline

- Introduction to Grid and Globus
- What is Grid Security? What makes it different?
- Current Grid Security
- Evolution to OGSA and Web services
- GT3 Implementation and Futures

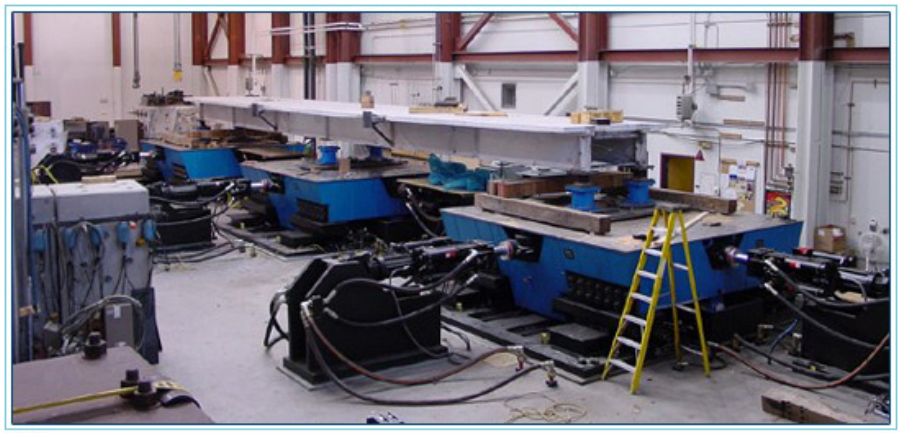
Why the Grid?
Origins: Revolution in Science



- Pre-Internet
  - Theorize &/or experiment, alone or in small teams; publish paper
- Post-Internet
  - Construct and mine large databases of observational or simulation data
  - Develop simulations & analyses
  - Access specialized devices remotely
  - Exchange information within distributed multidisciplinary teams



NEESgrid Earthquake Engineering Collaboratory



U.Nevada Reno

www.neesgrid.org

Remote Users (Faculty, Students, Practitioners)

Instrumented Structures and Sites

Laboratory Equipment

High-Performance Network(s)

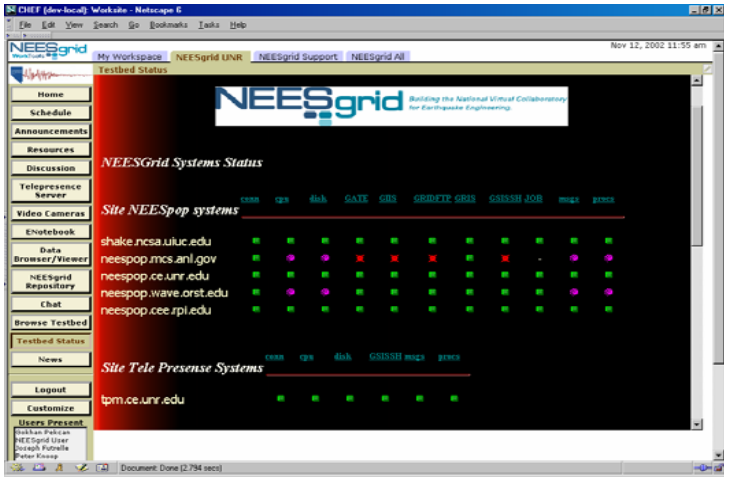
Field Equipment

Curated Data Repository

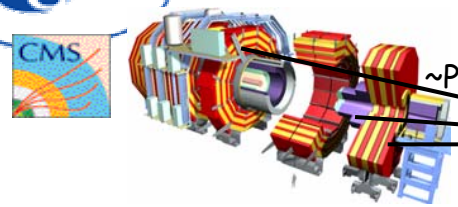
Global Connections (fully developed FY 2005 – FY 2014)

Laboratory Equipment (Faculty and Students)

Remote Users: (K-12 Faculty and Students)



LHC Data Distribution



~PBytes/sec

Online System

~100 MBytes/sec

1 TIPS is approximately 25,000 SpecInt95 equivalents

There is a "bunch crossing" every 25 nsecs.
There are 100 "triggers" per second
Each triggered event is ~1 MByte in size

Offline Processor Farm
~20 TIPS

~100 MBytes/sec

Tier 0

CERN Computer Centre

HPSS

~622 Mbits/sec
or Air Freight (deprecated)

Tier 1

France Regional Centre

Germany Regional Centre

Italy Regional Centre

FermiLab ~4 TIPS

~622 Mbits/sec

Tier 2

Caltech ~1 TIPS

Tier2 Centre ~1 TIPS

~622 Mbits/sec

Institute ~0.25TIPS

Physics data cache

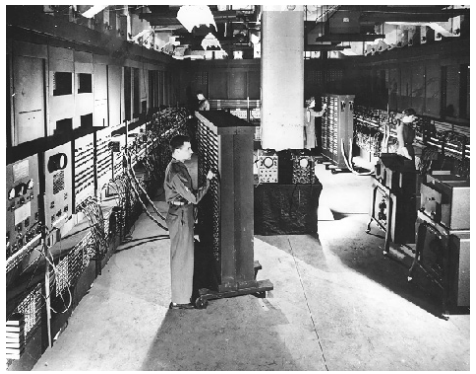
~1 MBytes/sec

Tier 4

Physicist workstations

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

Why the Grid?
New Driver: Revolution in Business



- Pre-Internet
  - Central data processing facility
- Post-Internet
  - Enterprise computing is highly distributed, heterogeneous, inter-enterprise (B2B)
  - Business processes increasingly computing- & data-rich
  - Outsourcing becomes feasible → service providers of various sorts
  - Growing complexity & need for more efficient management

What is the Grid?

- The Grid problem is to enable “coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations.” From *The Anatomy of the Grid*

- Grid = an emerging standard set of protocols and associated implementations that address the Grid problem

The Globus™ Alliance

Making Grid computing a reality

- Argonne, USC/ISI, EPCC, PDC, NCSA
- Close collaboration with many scientific and commercial Grid application and infrastructure projects
- Development and promotion of standard Grid protocols 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® software: Open source software base for building Grid infrastructure and applications

the globus alliance
www.globus.org

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**

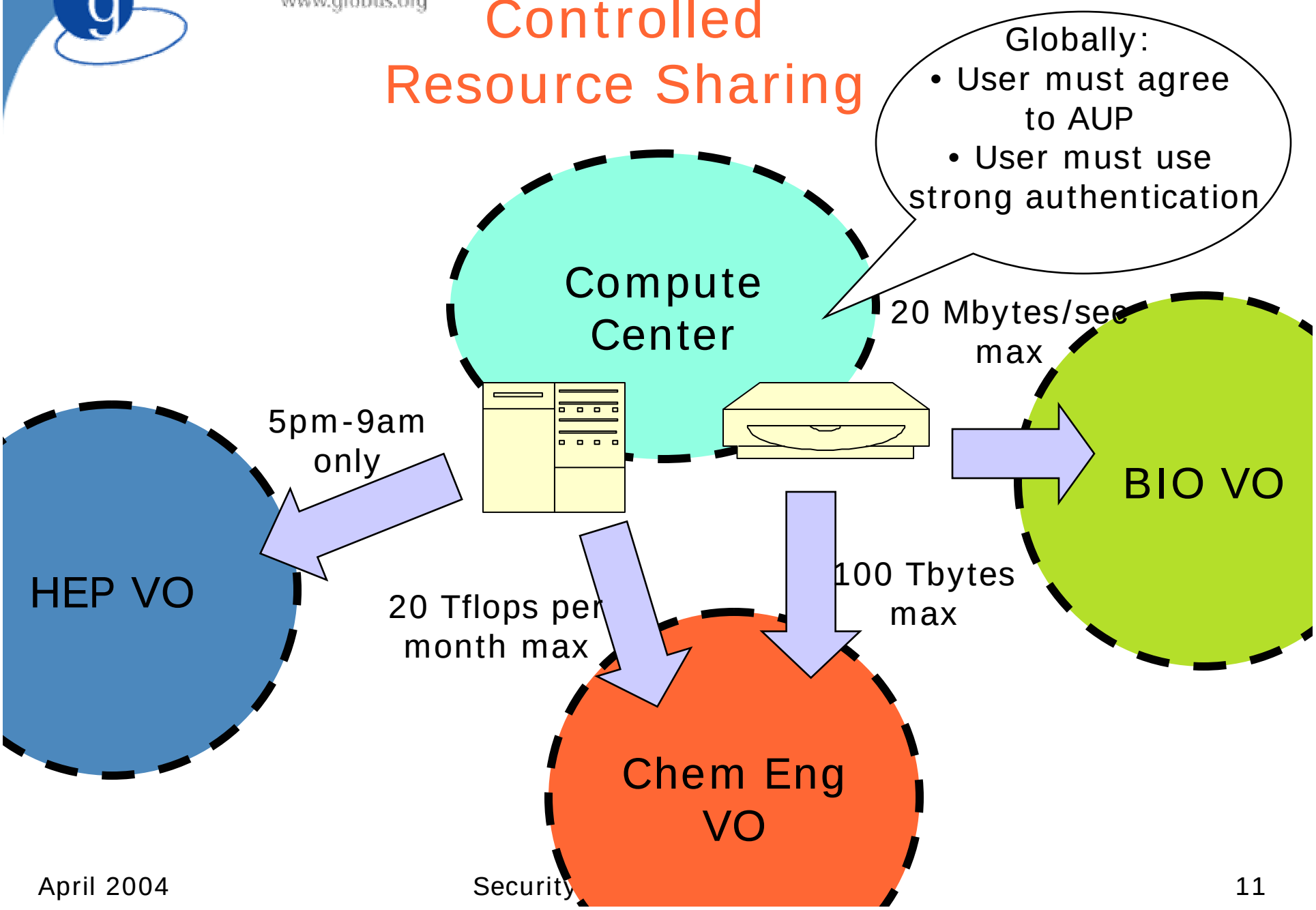
- So Grid Security is security to enable VOs
- What is needed in terms of security for a VO?

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

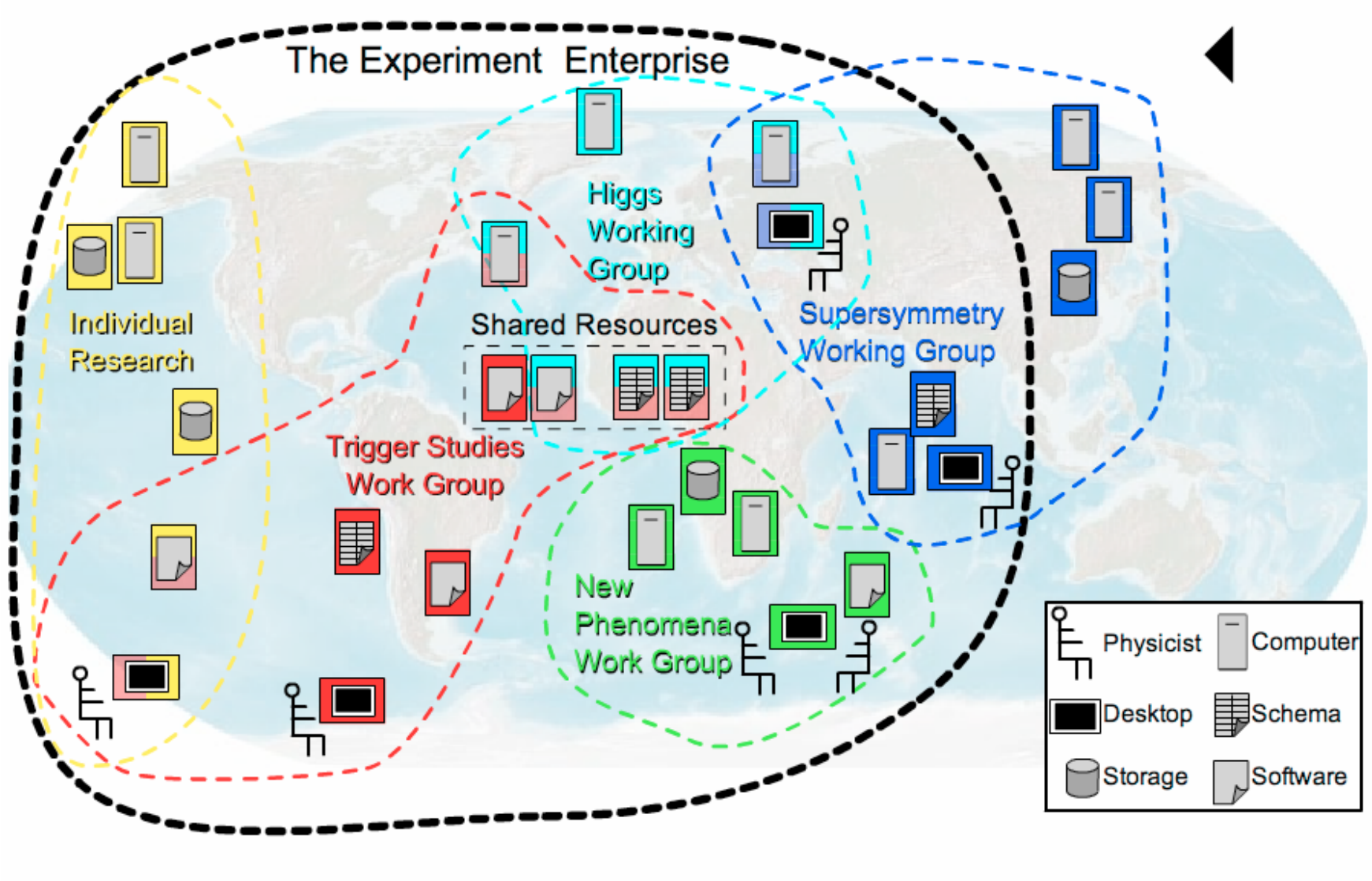
"...coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."

- 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

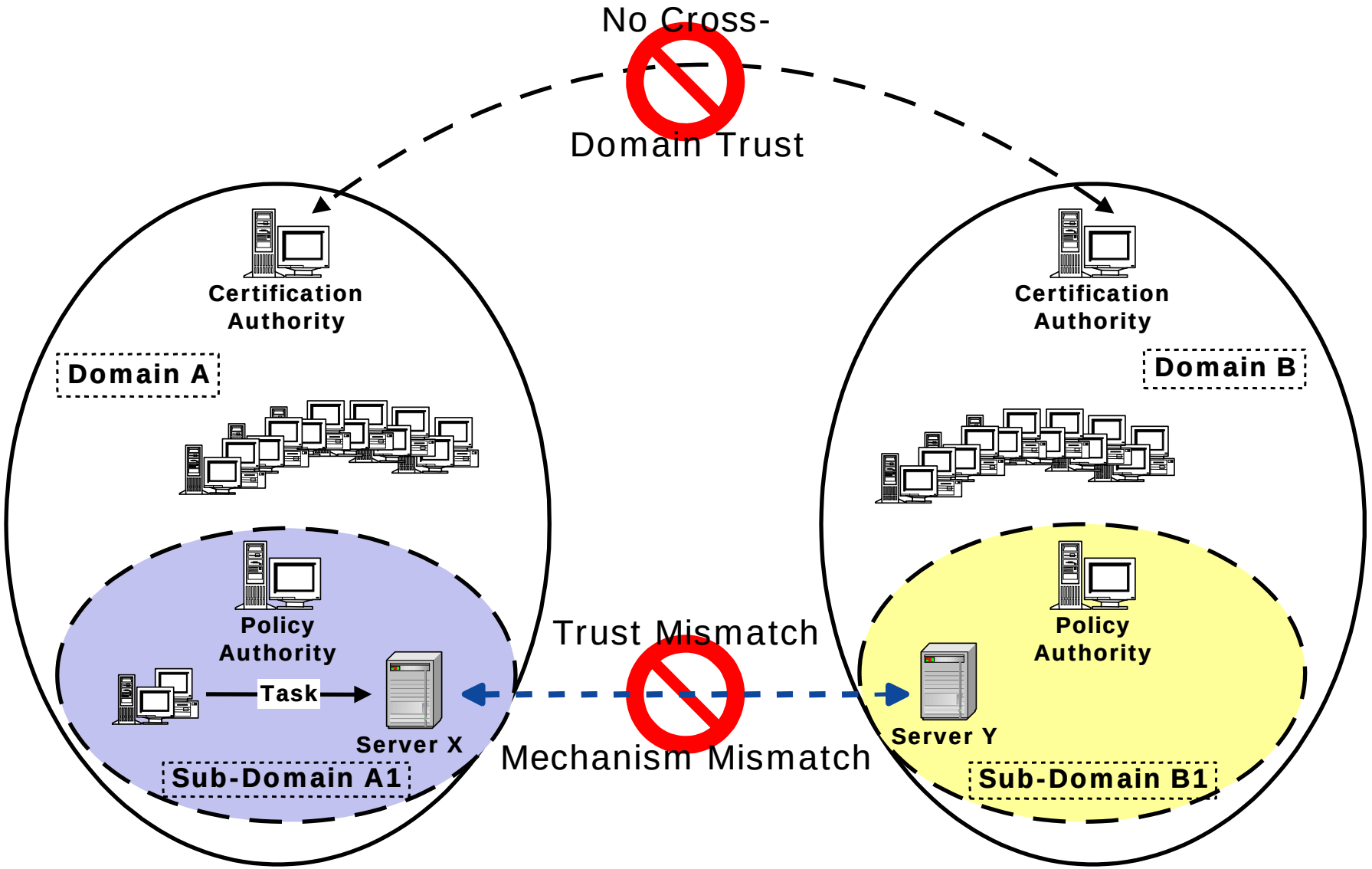
Multiple Organizations, Mechanisms, Policies

"...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


The Experiment Enterprise
Higgs Working Group
Shared Resources
Supersymmetry Working Group
Individual Research
Trigger Studies Work Group
New Phenomena Work Group
Physicist
Computer
Desktop
Schema
Storage
Software

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 vs WS-Security, X.509 vs. X.509 (different domains),
    - X.509 attribute certs vs SAML assertions

the globus alliance
www.globus.org

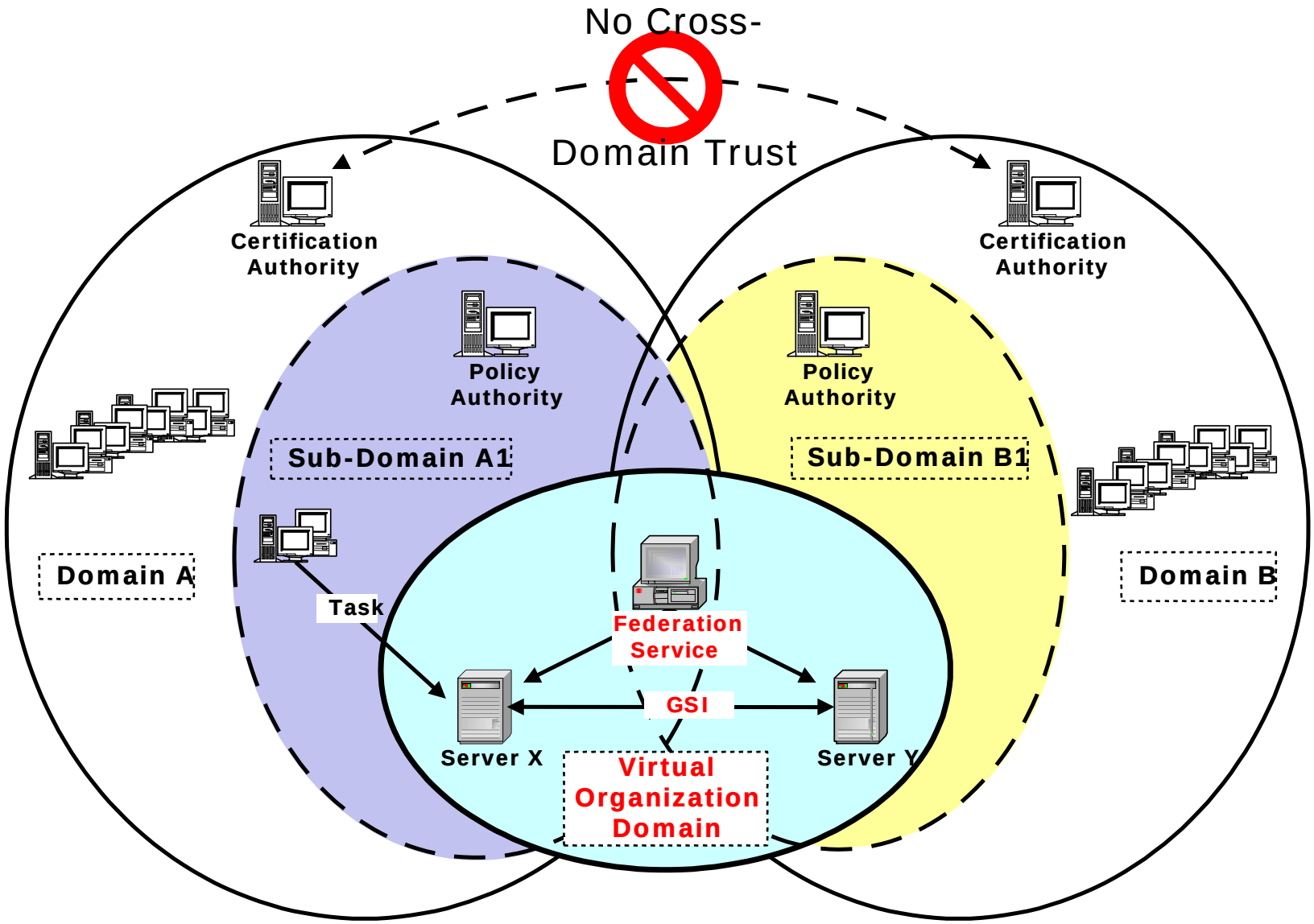
Why Grid Security is Hard...

- 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

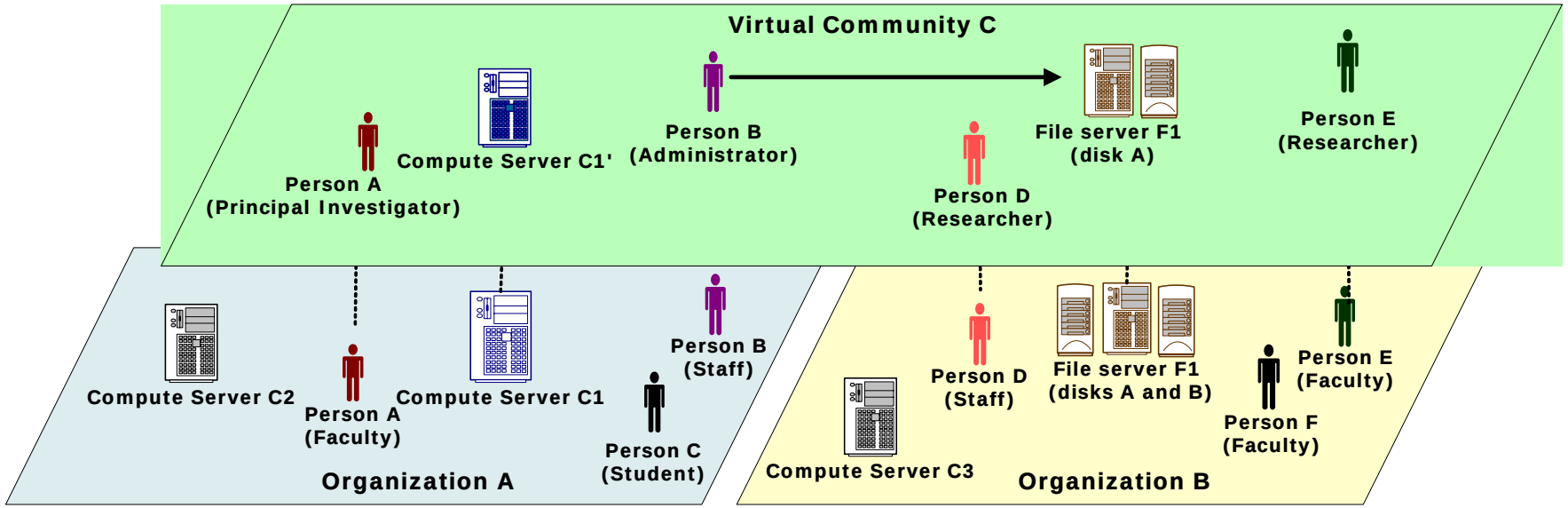
- Instead of setting up trust relationships at the organizational level …
  - Large overhead, slow adaptation, legalities
- … set up trust at the user/resource level
  - Leverage existing trust relationships
- VOs for multi-user collaborations
  - Federate through mutually trusted services
  - Local 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

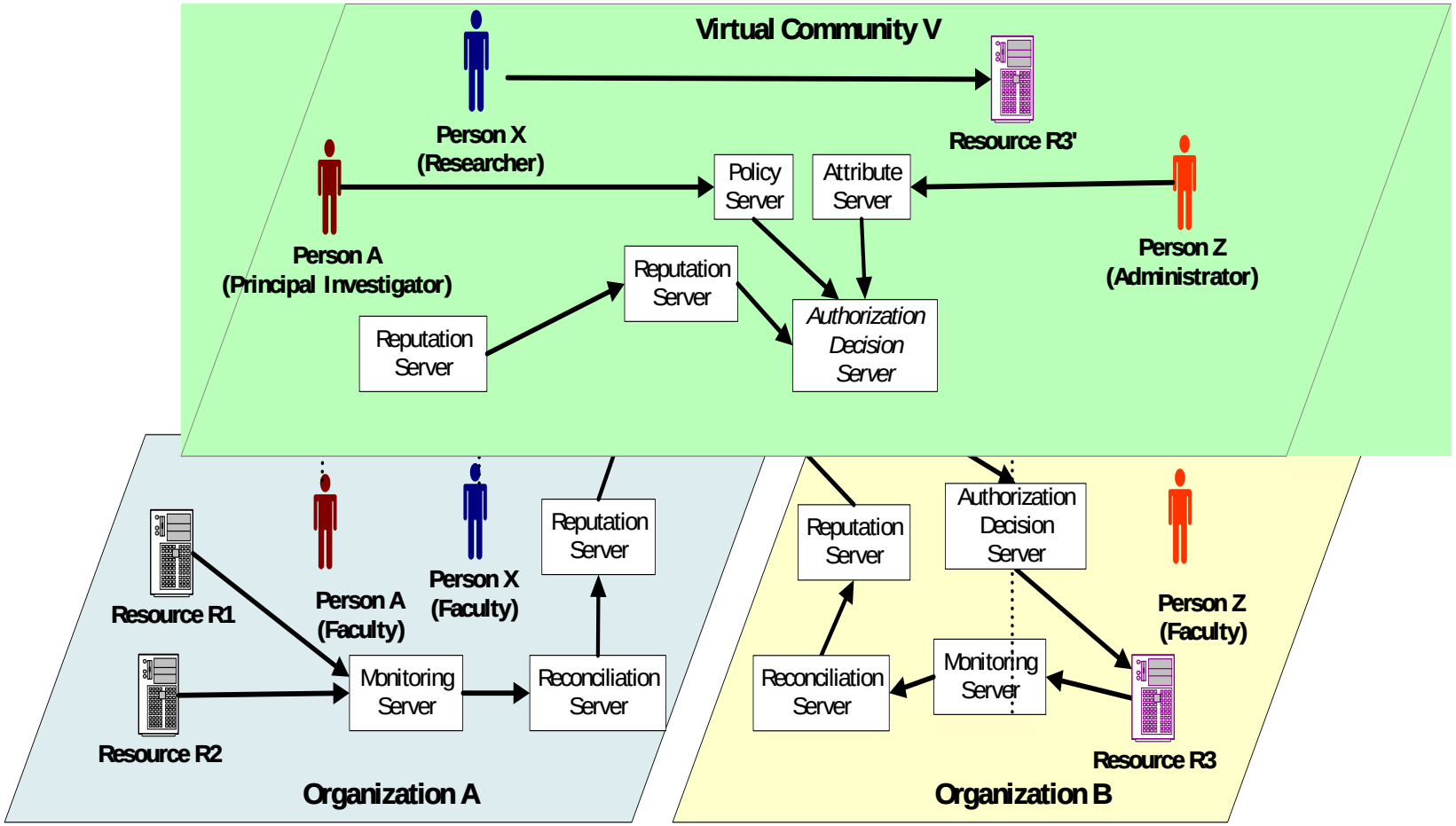


the globus alliance
www.globus.org

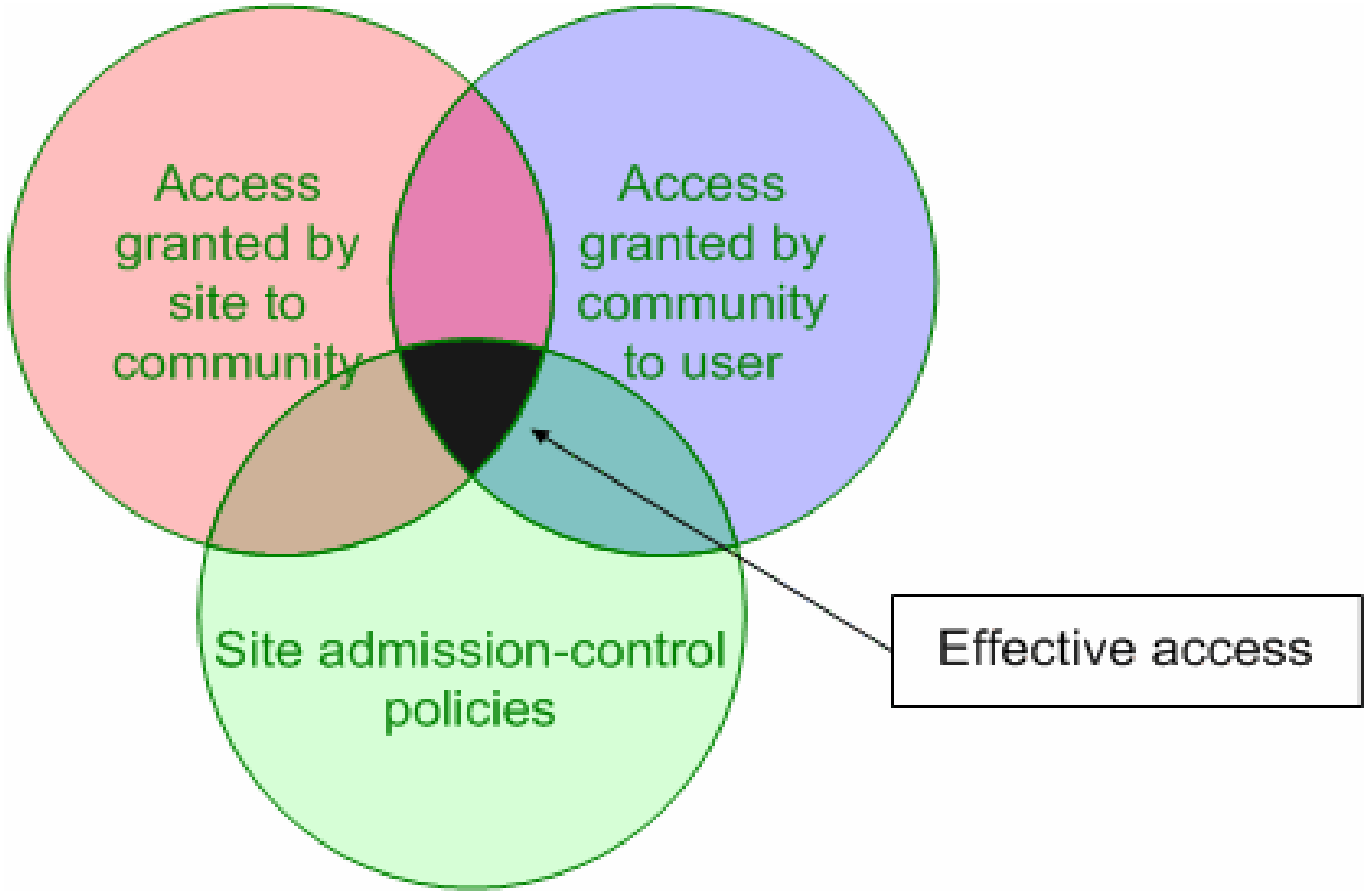
Virtual Organization Enables Access



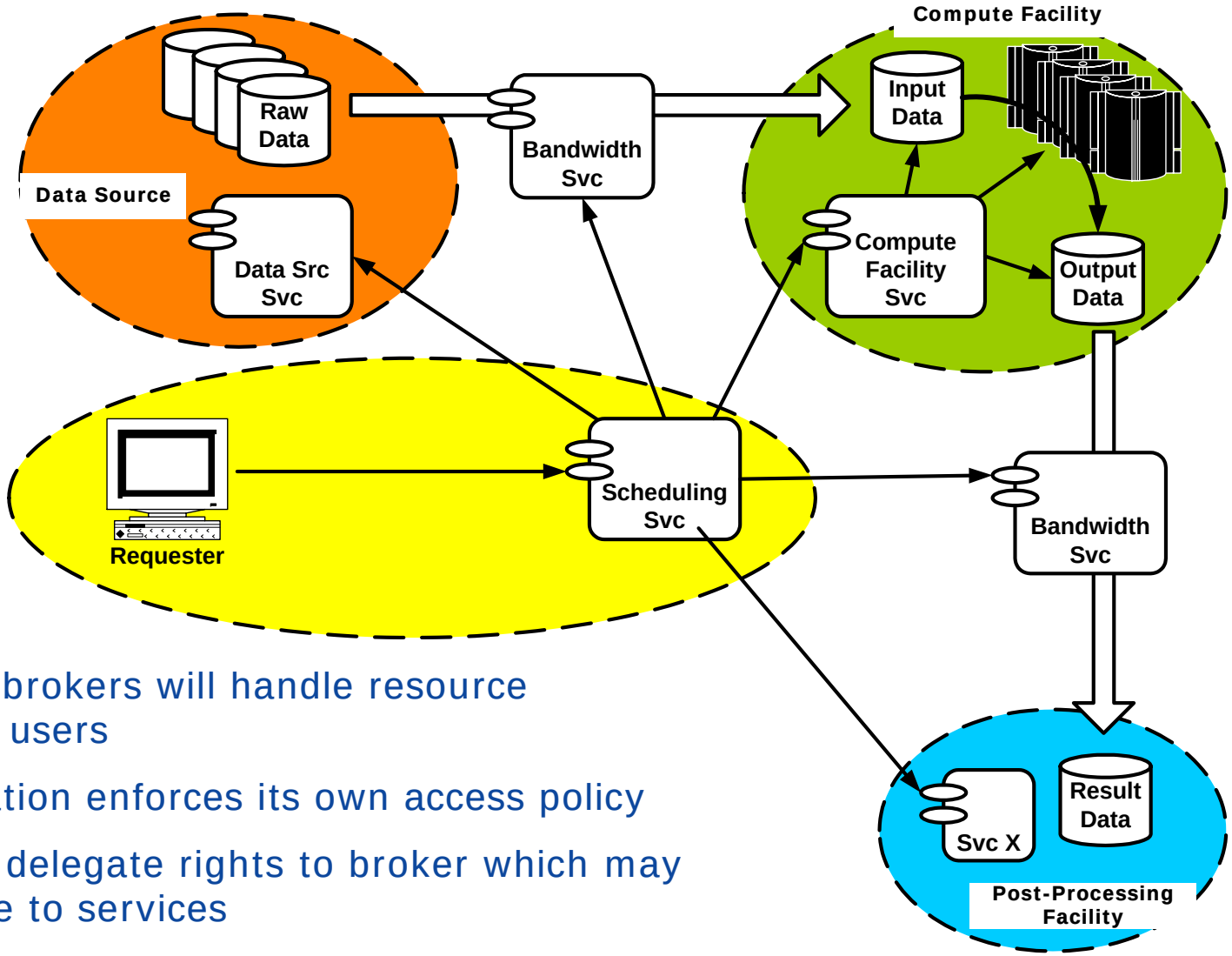
Building Trust through Reputation



Effective Policy Governing Access Within A Collaboration



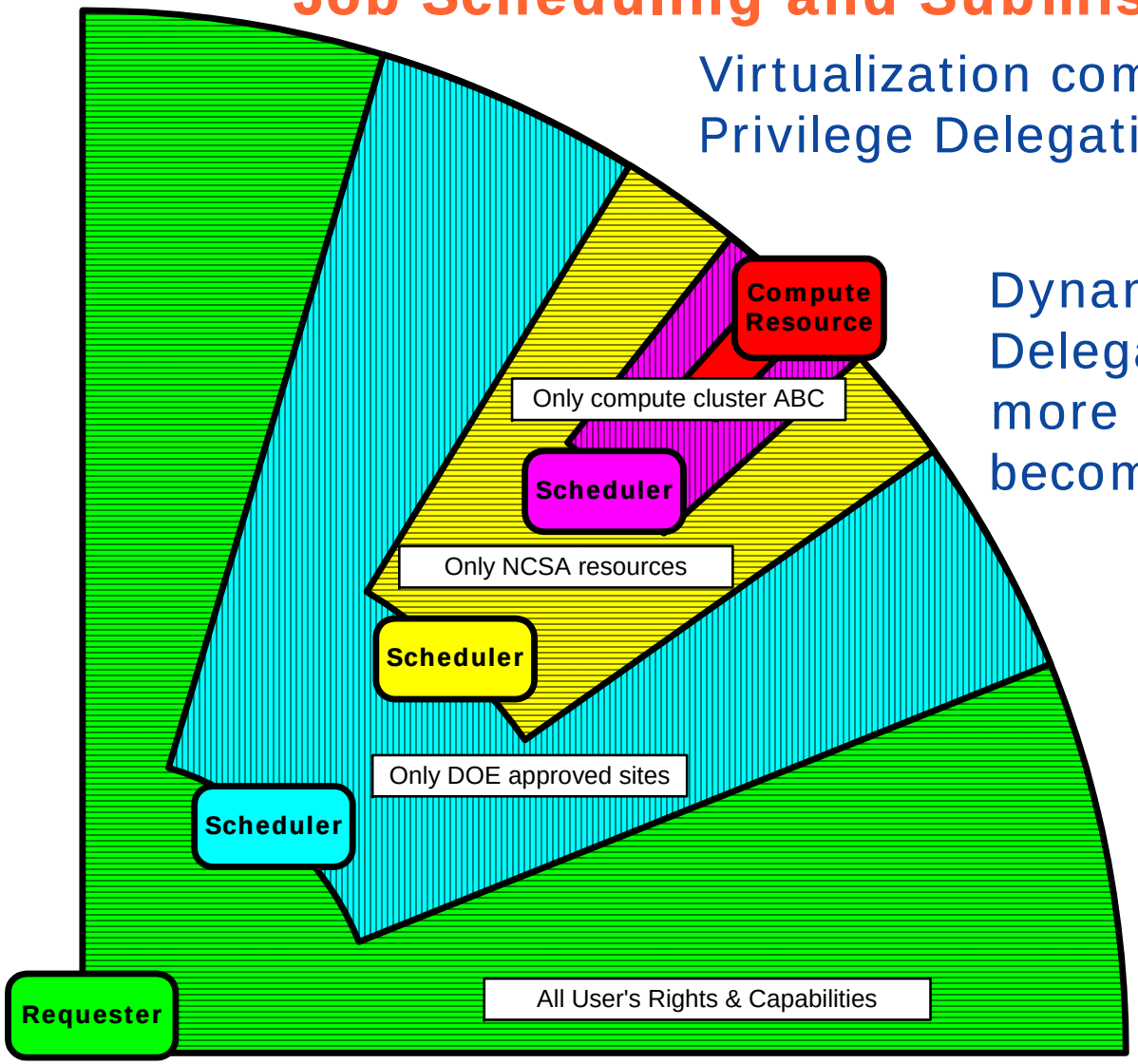
Security of Grid Brokering Services



- 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

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 with minimal 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.

the globus alliance
www.globus.org

Outline

- Introduction to Grid and Globus
- What is Grid Security? What makes it different?
- Current Grid Security
- Evolution to OGSA and Web services
- GT3 Implementation and Futures

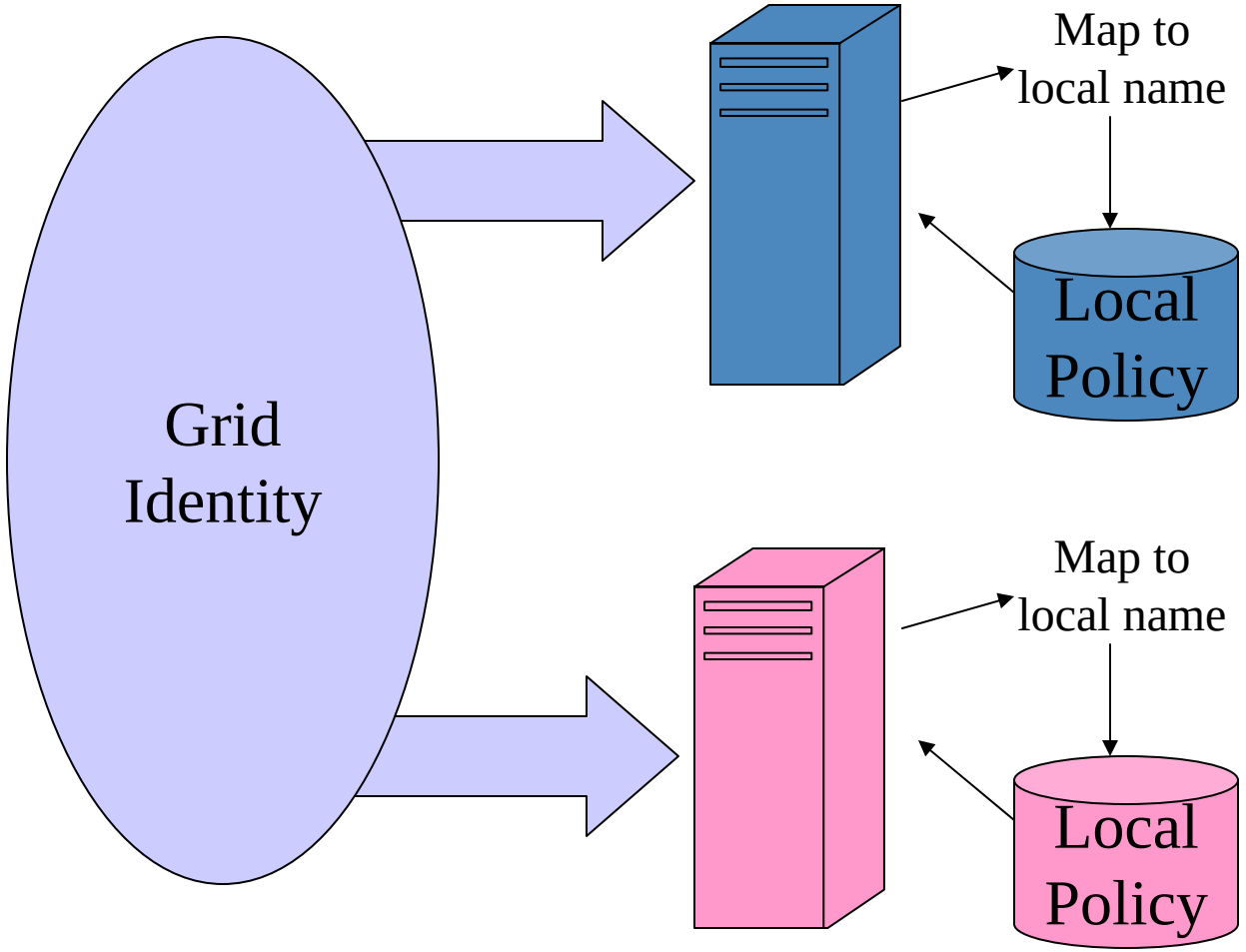
Grid Security Infrastructure (GSI)

- Based on standard PKI technologies
  - SSL protocol for authentication, message protection
  - CAs allow one-way, light-weight trust relationships (not just site-to-site)
- 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.

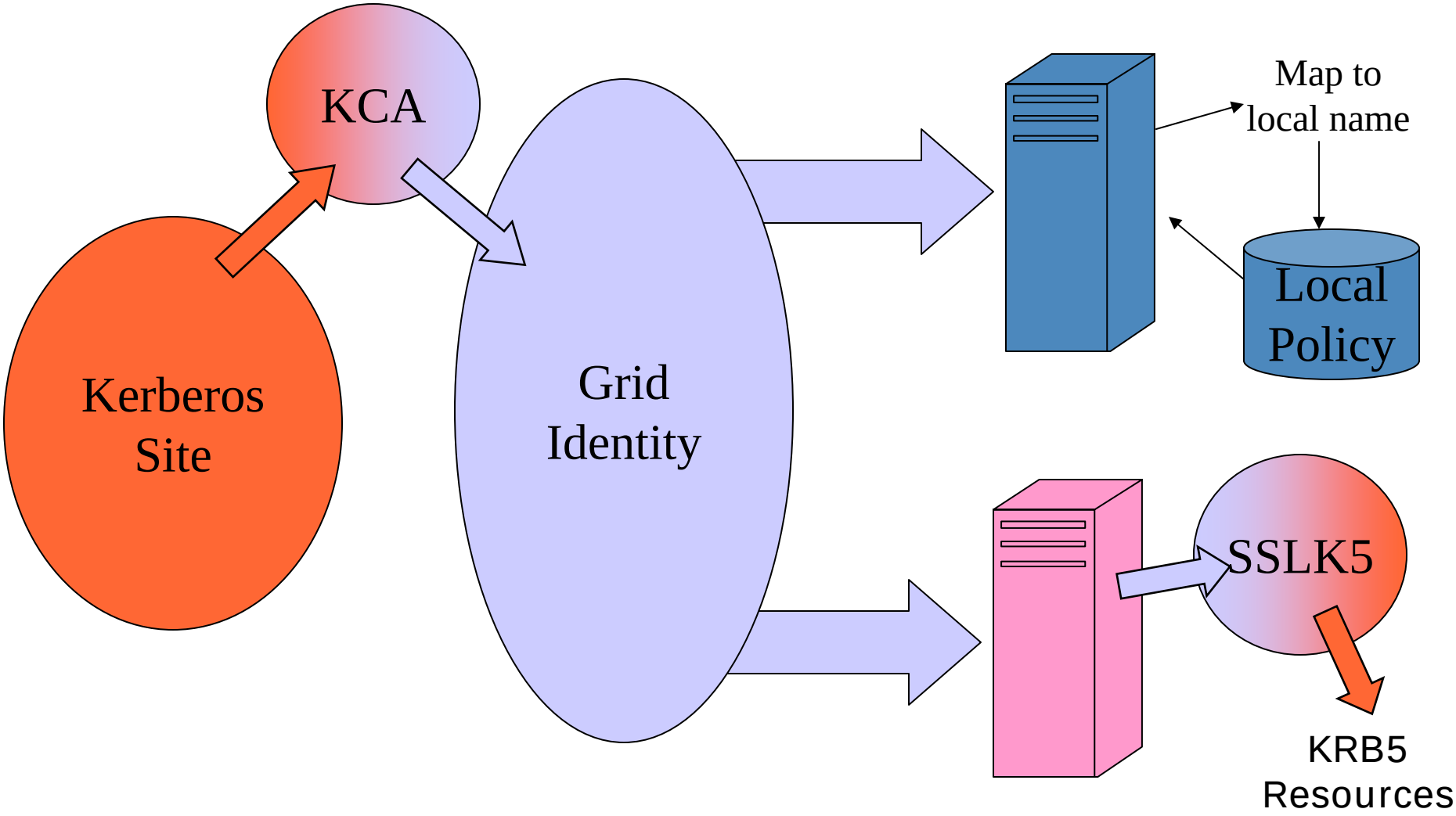
.



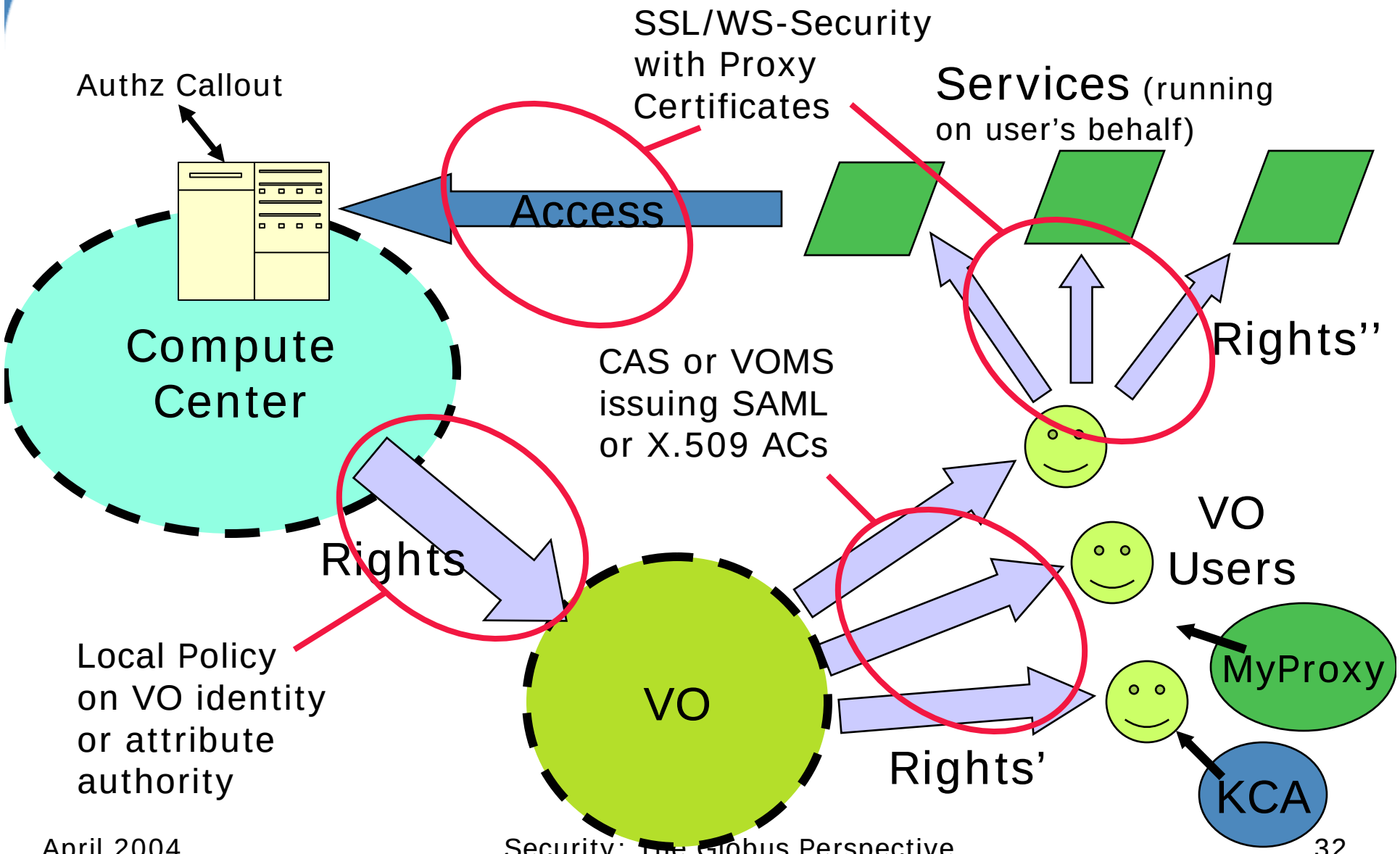
Kerberos to GSI Gateway

- 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



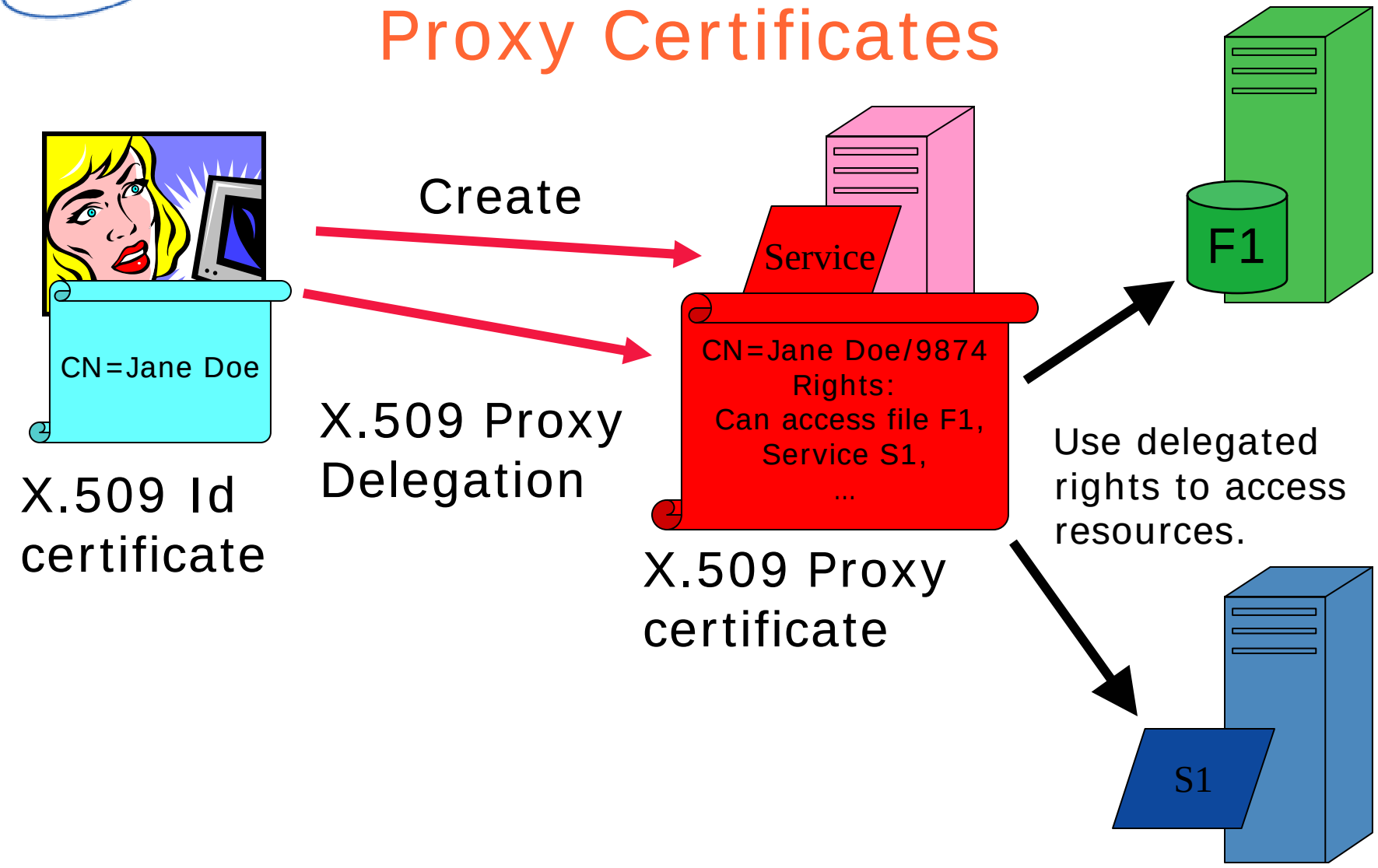
GSI Implementation



X.509 Proxy Certificates

- GSI Extension to X.509 Identity Certificates
  - On IETF RFC track
- 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

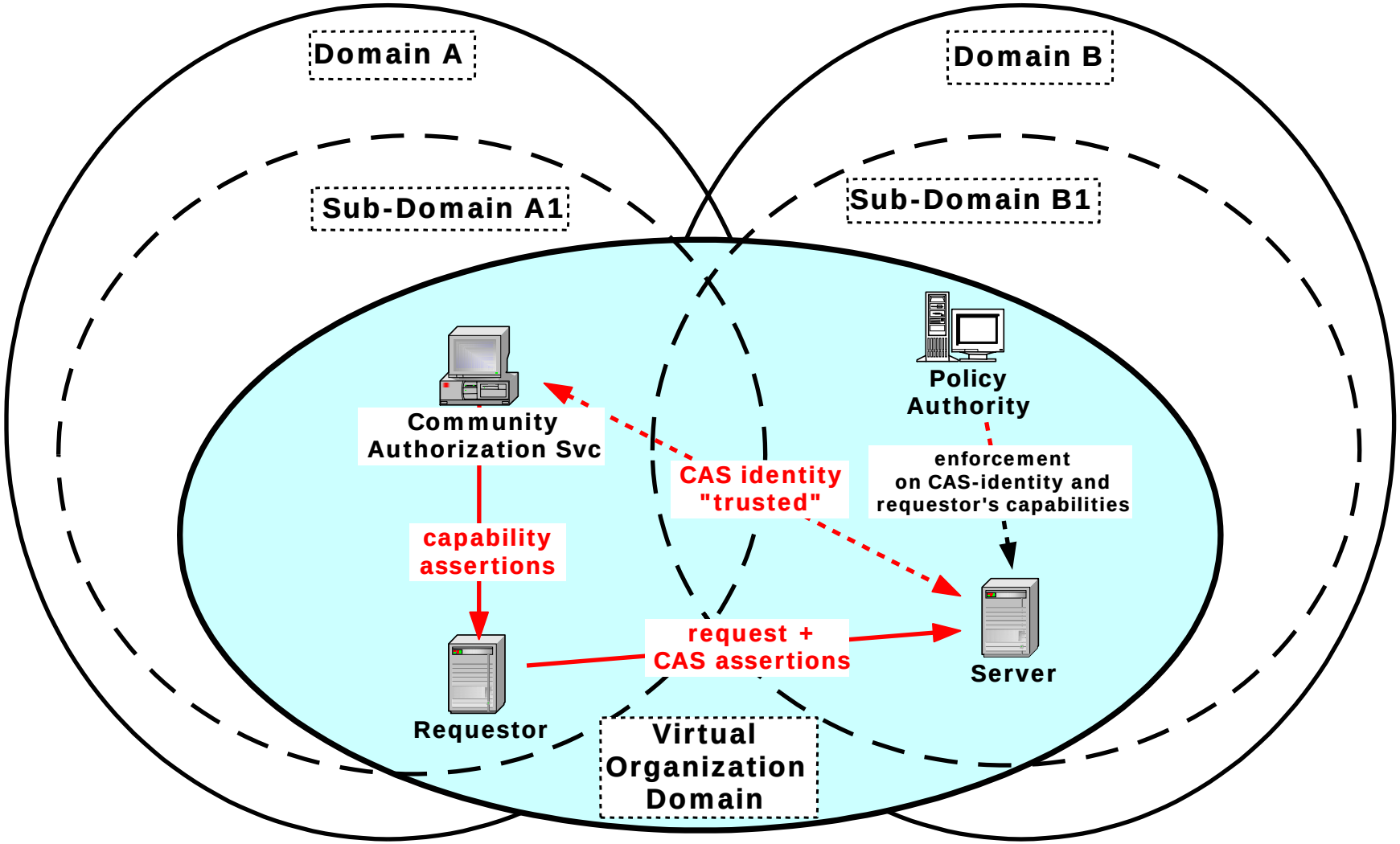


Community Authorization Service

- 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

the globus alliance
www.globus.org

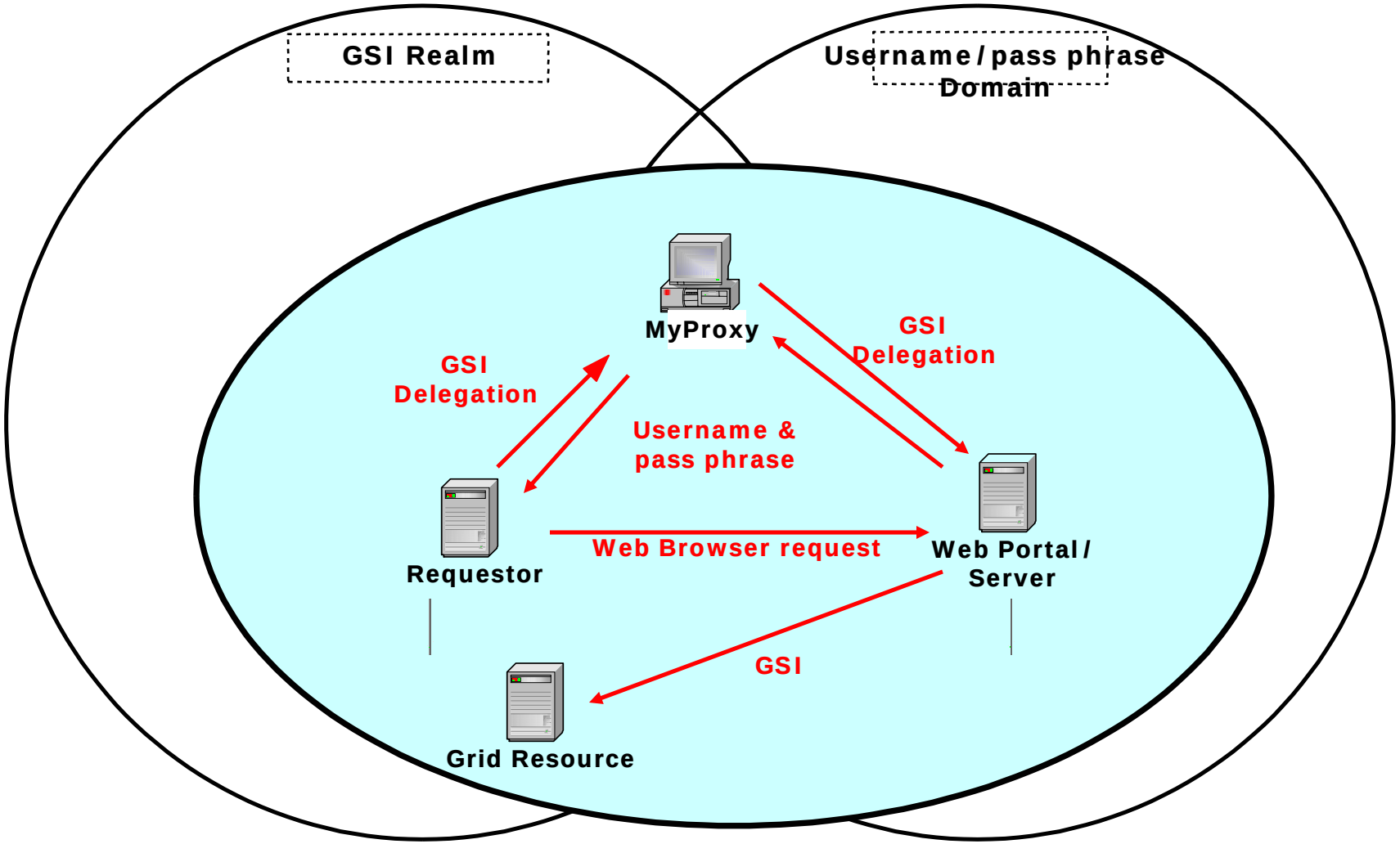
Community Authorization Service



MyProxy: Credential Wallet/Converter

- MyProxy allows users to store GSI credentials and retrieve them
  - With username/passphrase, one-time password, 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: Passphrase-X.509 Federation Service



the globus alliance
www.globus.org

Outline

- Introduction to Grid and Globus
- What is Grid Security? What makes it different?
- Current Grid Security
- Evolution to OGSA and Web services
- GT3 Implementation and Futures

Grid Evolution: Open Grid Services Architecture

- Goals
  - Refactor Globus protocol suite to enable common base and expose key capabilities
  - Service orientation to virtualize resources and unify resources/services/information
  - Embrace key Web services technologies for standard IDL, leverage commercial efforts
- Result = standard interfaces & behaviors for distributed system management built on Web services
  - Standardization within Global Grid Forum and OASIS
  - Open source & commercial implementations

the globus alliance
www.globus.org

OGSA Security Roadmap Goal

- Address the Grid Security Architecture Requirements

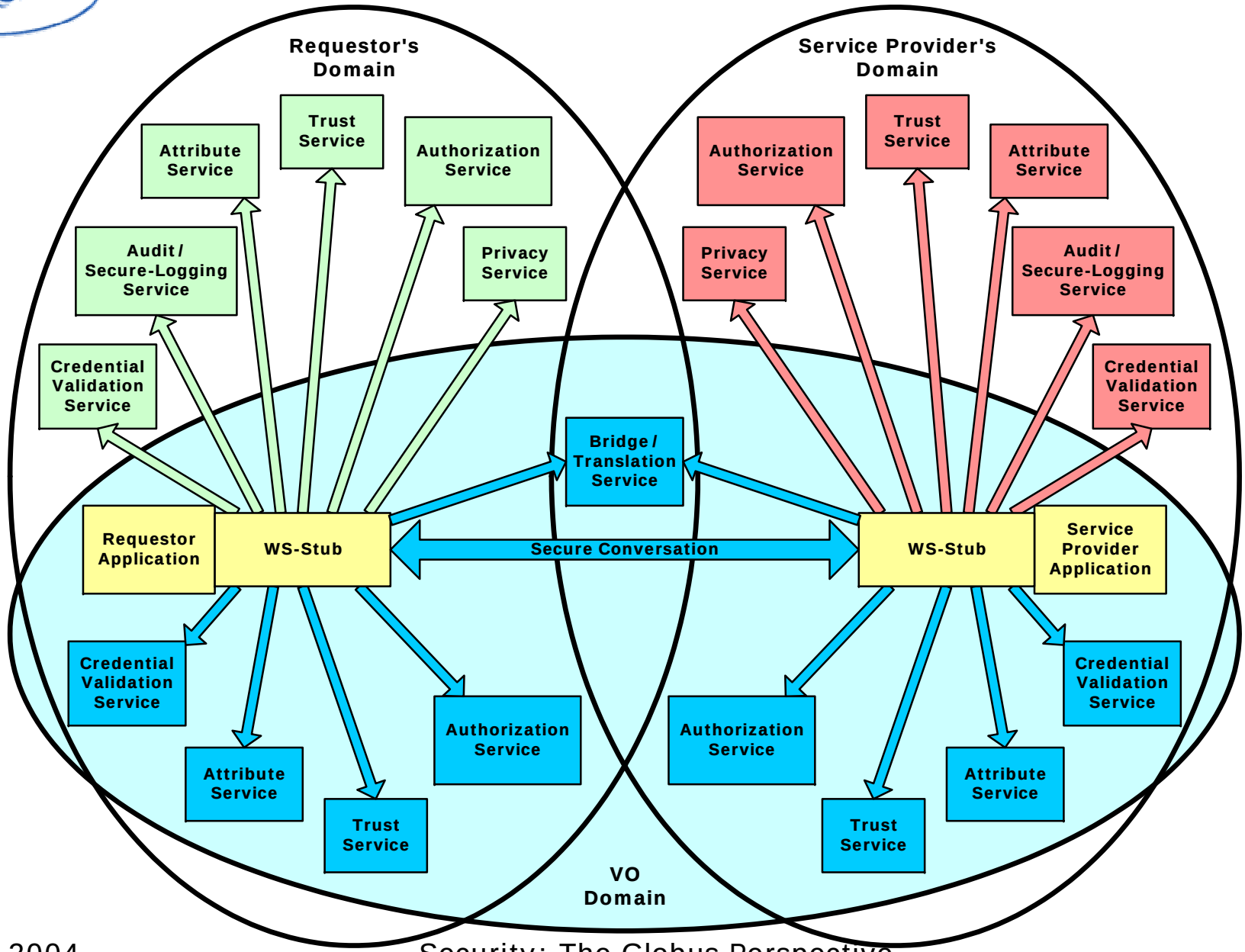
- **Make Implementations Possible**

- Address Interoperability
- Address Pluggability/Replaceability
- Address missing/late/insufficient Standards

"OGSA Security Roadmap"

submitted to GGF – co-authored with IBM

OGSA Security Services



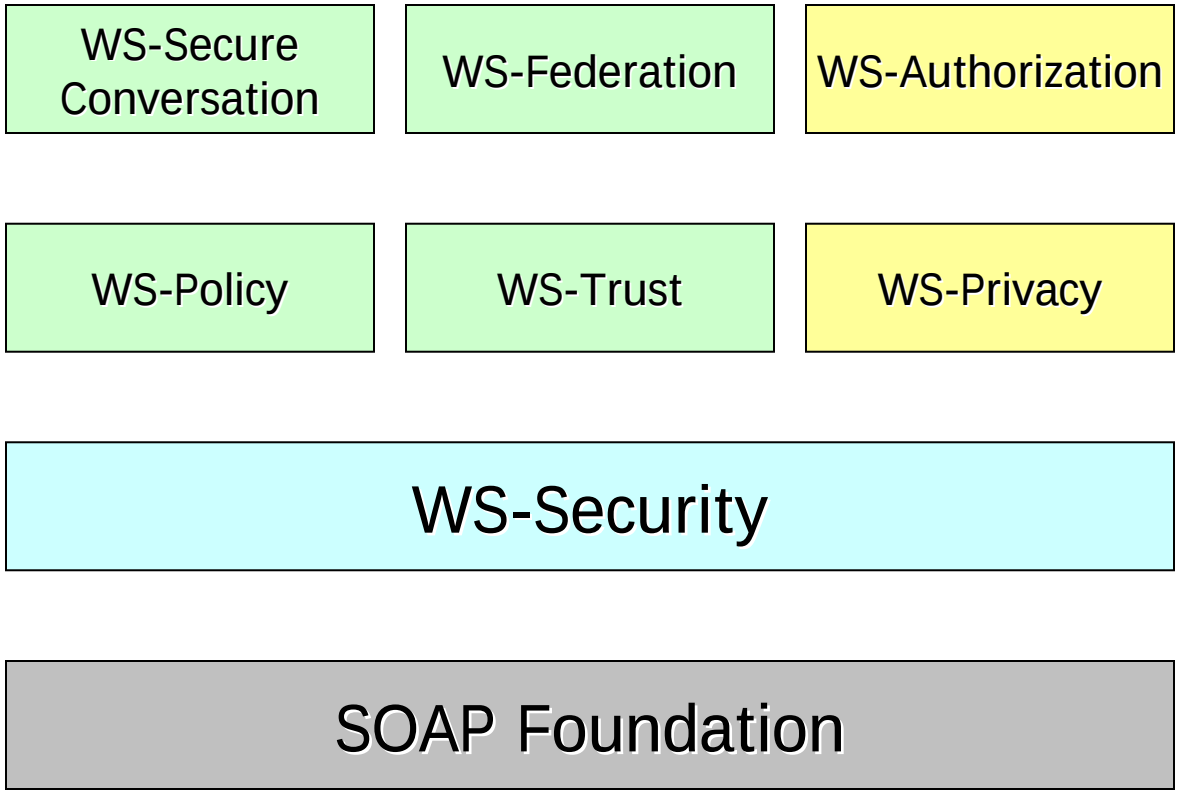
Leverage existing/emerging Security Standards

- WS-Security/Policy/Trust/Federation/ Authorization/SecureConversation/Privacy
- XKMS, XML-Signature/Encryption, SAML, XACML, XrML

- But…
  - Need to OGSA'fy
  - Need to define Profile/Mechanisms
  - Need to define Naming conventions
  - Need to address late/missing specs
  - Support for delegation, transient services

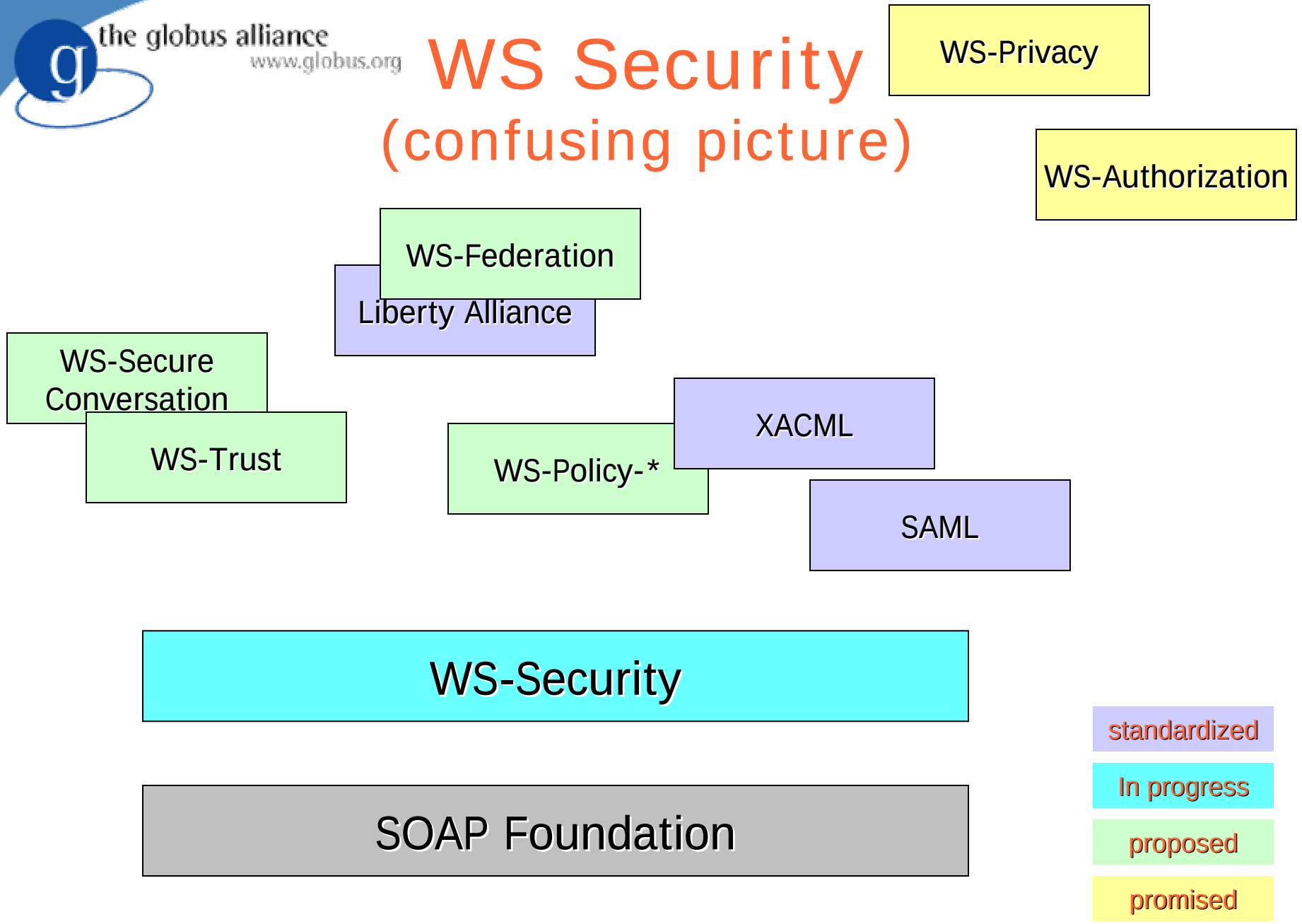
the globus alliance
www.globus.org

WS Security
Current/proposed WSS-specs



the globus alliance
www.globus.org

WS Security (confusing picture)



How WS Security fits...

- WS-Security: basic secure message primitives
- WS-Trust/SAML: basic secure protocol/assertion primitives
- Plus WS-Policy/XACML/XrML for expressing security constraints
  - What credentials (Kebreros, GSI) are accepted and preferred
  - Encryption supported? Required? Rejected?
- WS-Authorization/XACML/XrML for managing authorization data
  - e.g. in CAS
- WS-Privacy (?) for managing privacy

Concerns about WS Security Specs

- Slooow submission & standardization of specs
  - publish some specs, freeze the industry, and wait, wait, wait... until momentum is lost (?)
- IP and RF and RAND
  - Positive: most wss specs are submitted as RF
  - Clarifications take too long
  - Too many vendors involved with different T&Cs
  - Maybe authoring companies synchronize their lawyers and have single contracts...

the globus alliance
www.globus.org

OGSA Authz Goals

- Build on existing WS standards
  - SAML, XAMCL, WS Security Suite, XrML, etc.
- Support multiple mechanisms
  - But specify set for interoperability
- Remove Authz from application
  - Allow deployer to select
- Enable VO-driven policies
  - Limited delegation

SAML and XACML

- Standards from OASIS
- SAML looks good for assertions
- XACML as language for policy exchange?
- Issues:
  - Don't fit nicely together (NASA work).
    - SAML 2.0 will hopefully help.
  - XACML delegation of rights?

Remove Authz from Applications

- Allow deployment-time selection of supported mechanisms and policies
- OGSA resource virtualization allows for policy on application-independent operation invocation
- Place as much security functionality as possible into sophisticated hosting environments

the globus alliance
www.globus.org

Outline

- Introduction to Grid and Globus
- What is Grid Security? What makes it different?
- Current Grid Security
- Evolution to OGSA and Web services
- GT3 Implementation and Futures

What's actually in GT3?

- Leveraging SOAP, WS-Security (XML-Signature, XML-Encryption) for wire protocol
  - Practical implementation of existing standards
- Using our implementation of WS-SecureConversation
  - Designed before public specification
  - Still doing SSL handshake, just doing it over SOAP
  - Practical implementation of necessary pre-standards
- Set up context and then use WS-Security
- (recently published WS-Security-Kerberos includes patterns that we may be able to use...
  but not standardized and depends on WS-Trust/SecureConversation which are not standardized...when do we switch?)

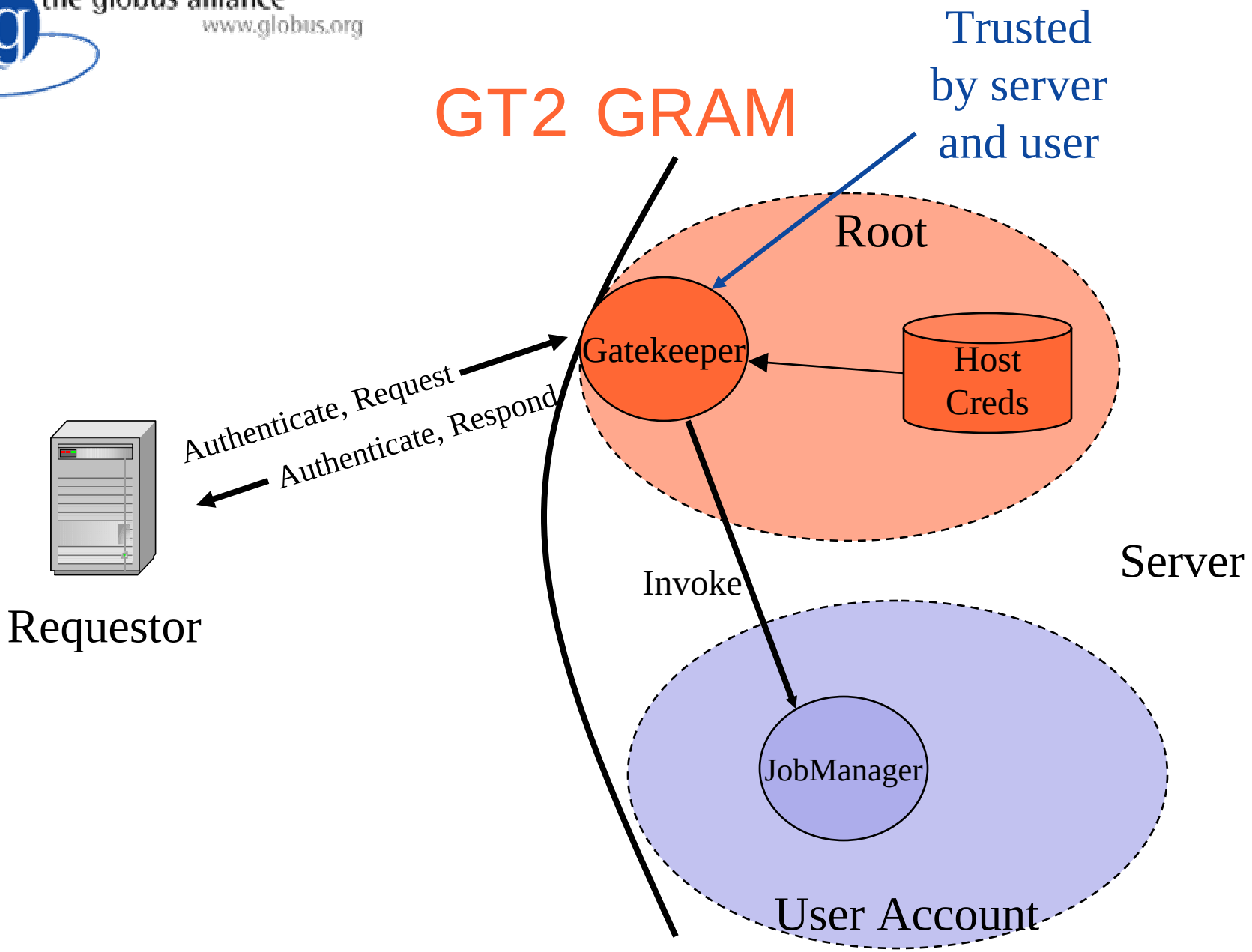
GT3 Secure Conversation

- Based on GT2's TLS/GSSAPI implementation
- Based on a poor-man's "interpretation" of WS-Trust/WS-SecureConversation specs plus XML-Signature/XML-Encryption/WS-Security
- Waiting for WS-Trust & WS-SecureConversation & WS-Kerberos specs to be submitted to standards body
- Need a standardized message-layer, session-based authentication and key-exchange protocol
  - Maybe a GGSAPI-like equivalent, based on WS-Trust/WS-SecureConversation/XML-Signature/ XML-Encryption/WS-Security ?
- Work in GGF's OGSA-Security on hold…

the globus alliance
www.globus.org

Least Privilege

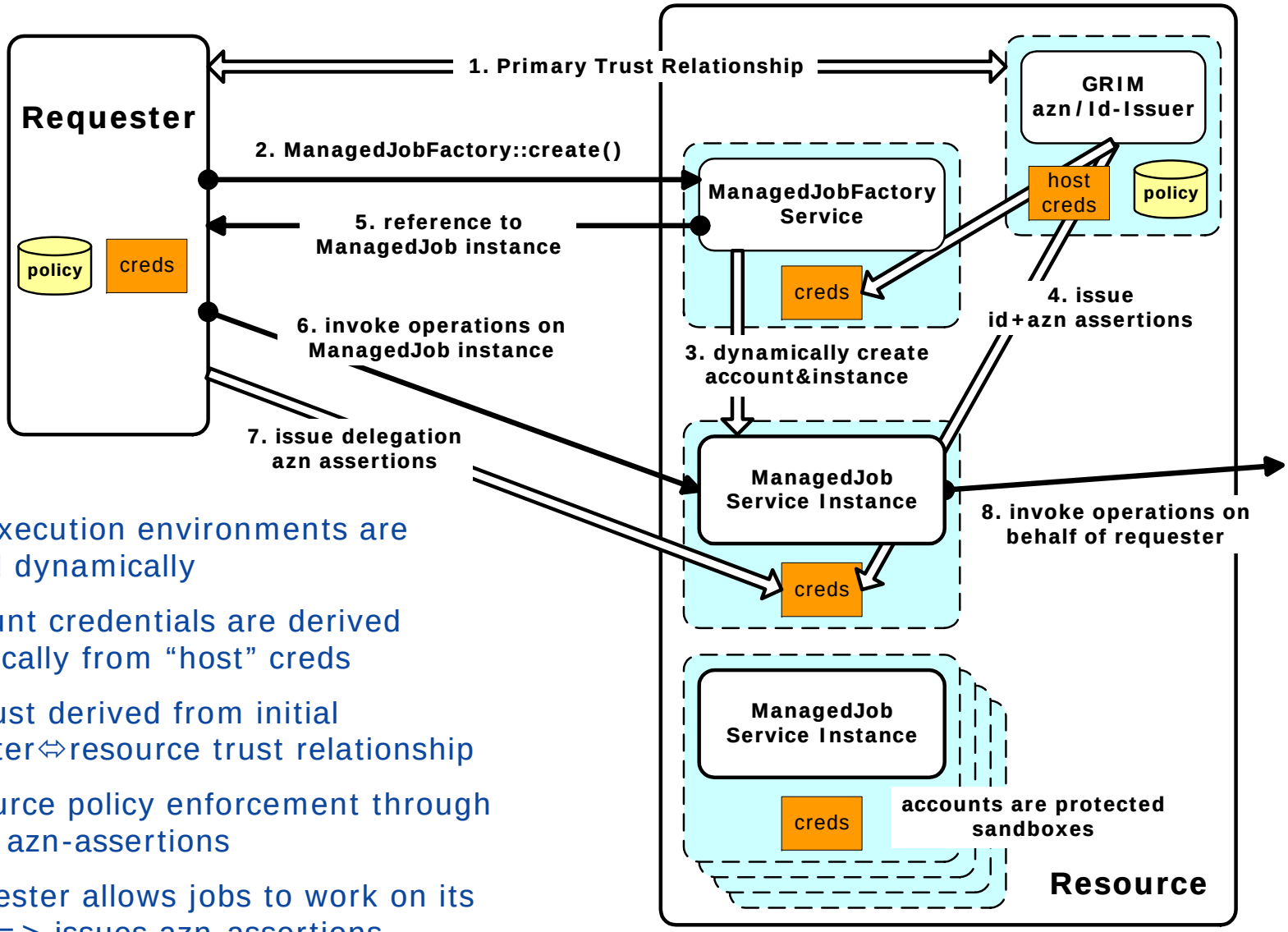
- In Globus Toolkit implementation we follow least privilege model
  - All code only has smallest amount of privileges required to do it's job
- In GT2 model, the Gatekeeper was the privileged piece of GRAM
  - Had all privileges on local system
  - Also acted as trust end-point for user by virtue of having access to host keys


GT2 GRAM
Trusted by server and user
Root
Gatekeeper
Host Creds
Authenticate, Request
Authenticate, Respond
Requestor
Server
Invoke
JobManager
User Account

GT3 Least Privilege Model

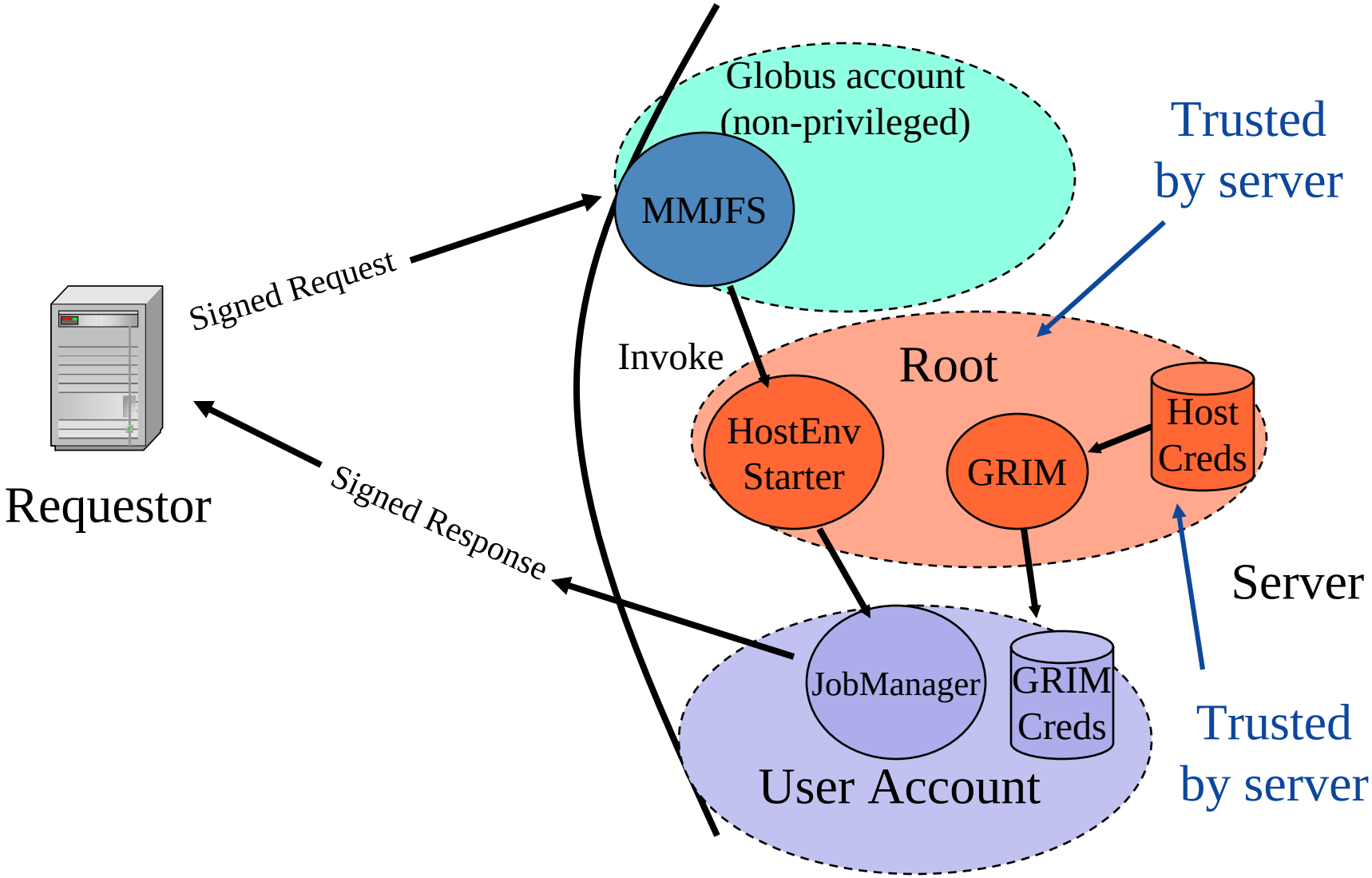
- GT2 Model good, but
  - Gatekeeper accepts network connections - possible to attack
  - Gatekeeper could be broken down into smaller pieces
- GT3 model
  - Make network services non-privileged
  - Break up privileged pieces into smallest chunks of functionality with smallest privileges - 2 setuid programs:
    - **User Hosting Environment starter** - starts pre-configured hosting environment for user
    - **GRIM** - gets credentials for accounts to use to authenticate to requestors

GT3's Resource Management



- Job execution environments are created dynamically
- Account credentials are derived dynamically from "host" creds
- All trust derived from initial requester⇔resource trust relationship
- Resource policy enforcement through GRIM's azn-assertions
- Requester allows jobs to work on its behalf => issues azn-assertions

GT3 GRAM


Globus account
(non-privileged)
MMJFS
Trusted
by server
Signed Request
Invoke
Root
HostEnv
Starter
GRIM
Host
Creds
Requestor
Signed Response
Server
JobManager
GRIM
Creds
User Account
Trusted
by server

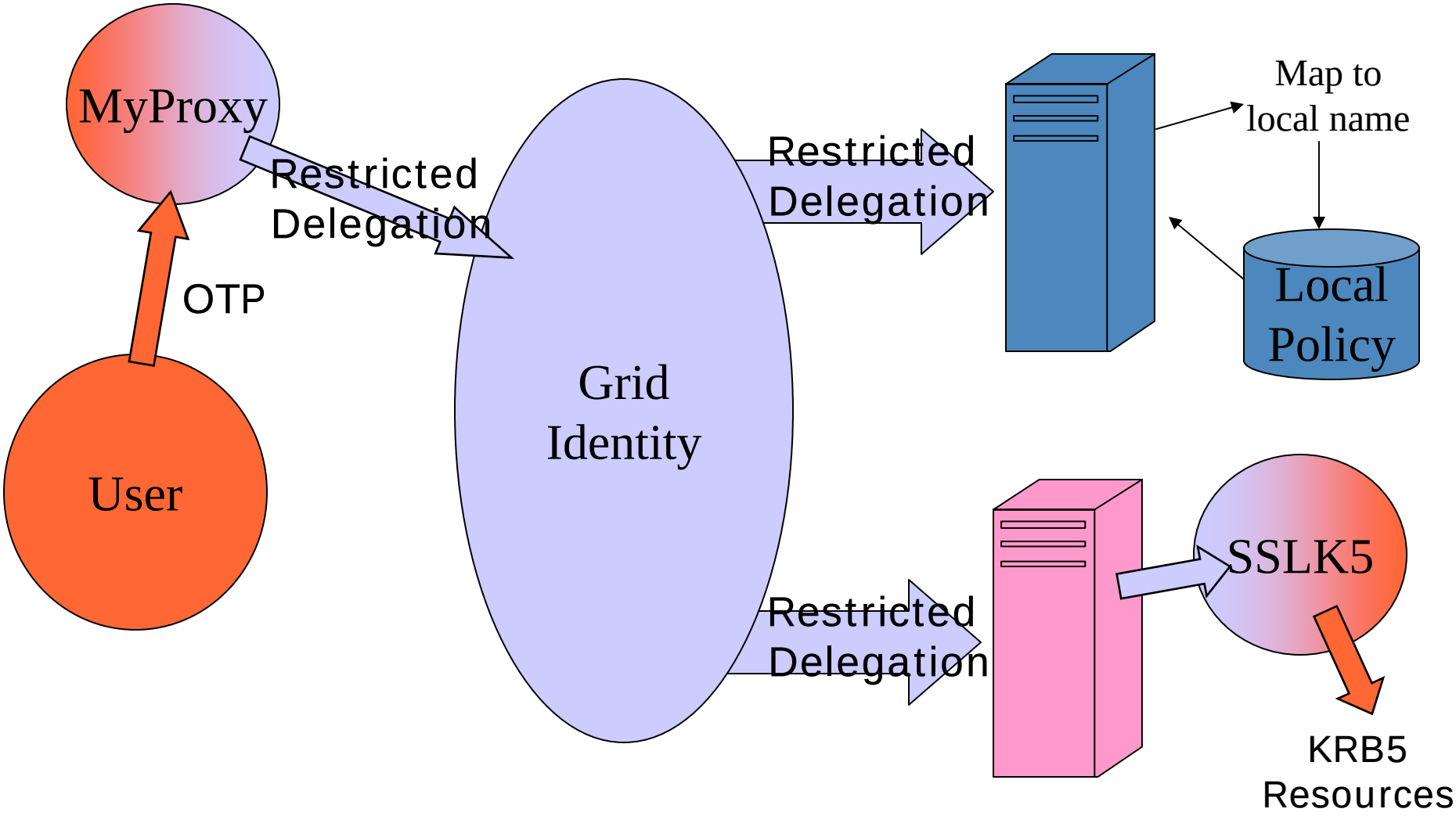
Dynamic Resource Management

- Dynamic account/sandbox creation
  - X.509 identity registration procedure doesn't work…
  - Identity assertion not very useful…
- Newly created key pair are "the" identity creds
- Currently use proxy-certs to issue azn-assertions
  - GRIM asserts that requester can be trusted by account
  - GRIM asserts account can be trusted by requester
  - Requester asserts account can work on behalf of requester
- Future: XACML policy statements wrapped in SAML authorization assertions on bare keys issued by more permanent identities like host-identity and requester
- Leverage on GGF's OGSA-Authorization WG work

Hacked Compromised Systems: Learn to Live With It…

- Seems impossible to keep systems up-to-date and safely configured
- Minimize consequences of compromise
  - No long-term secrets on workstations
    - Passphrase protected not good enough
  - No typing-in of any long-term passwords
    - Keyboard sniffers
  - Minimize delegated rights to reduce exposure from compromised temporary credentials

One Time Passwords and Restricted Delegation



OGSA/GT3 Security Futures (1)

- Authorization
  - Includes communicating/sharing/matching of authz-policies and capabilities
- “Secure” Password/One-Time-Password authentication/key-exchange integration
- VO Security Policy life-cycle framework
  - Leverage authz policy work
- Message-based, context-based pure XML security protocols
  - Seems a missing link…(SSL/GSI will work for now)

OGSA/GT3 Security Futures (2)

- Integration of Group authentication/key-exchange protocols
  - Going from 2 parties to N parties should be “seamless”
- Securely route through firewalls/network-hurdles
  - Tackle the firewall/NAT traversal issues transparently in the runtime
- On-line Security “Policy” Registries
  - Policies, capabilities, attributes, assertions: we need real-time registries…
- Secure Logging and Audit
  - Another undefined, unstandardized missing link… while the requirements are there!

Conclusion

- Grid's requirements maybe few years ahead, but everybody will face same challenges soon
  - Few "new" distributed computing requirements…
- Our security requirements are conceptually 1-2 levels above what is available now as specifications, standards and open source
  - Ideally, we want to be end-users of WSS not plumbers…
- The standards circus is very worrisome
  - And distracting and time consuming…
- But Globus Toolkit provides a working, evolving implementation for "secure" Grid protocols
  - Downloaded 100k+ times already (www.globus.org)