GENI Clearinghouse Federation

Corporation for National Research Initiatives

GPO Clearinghouse Requirements

- A clearinghouse
  - Should minimize the number of trust relationships required between **researchers** and **aggregates** to perform any transaction
  - Should log transactions and, by using the logs, enable **forensics** and **kill-the-experiment** functionality
  - Should enforce global policies
- Note
  - The requirements do not talk about implementing registries, slice authorities or component/aggregate managers

Cluster Member Clearinghouse Requirements

- As per cluster members (based on ongoing discussion), a clearinghouse
  - Should provide functionality such as authentication, authorization, registry services, policy enforcement systems
  - Should not bundle the functionality into a single (logical) component/service, but provide the clients a way to use the functionality separately on an as needed basis
- Note
  - Need for including slice authority and component/aggregate manager functionality in the clearinghouse is still being discussed

ProtoGENI Clearinghouse

- ProtoGENI clearinghouse is a single service that
  - Provides registration and resolution of metadata associated with users, slices, component managers, slice managers
    - Does not provide search capability on the metadata
  - Provides shutdown of a slice (experiment)
  - Authenticates and authorizes the client for all service requests based on assigned privileges (certificates and credentials)
- Note
  - Slice Authority and Component Manager functionality is defined separately

Our Clearinghouse Goals

1. Minimize the number of trust relationships required between researchers and aggregates to perform any transaction

2. Provide authentication, authorization, registration, resolution, and discovery services on user records, slices, resources, components, aggregates, component/aggregate managers, and slice managers
   - Leave the Slice Authority and Component/Aggregate functionality to individual clearinghouses

3. Provide the above services discretely by not bundling the services into one big service
   - That is, allow intermediary clients to bundle only required services to offer value-added services to end users

Our Clearinghouse Goals - Cont'd

4. Allow fine-grained administration with distributed access
   - Fine-grained administration implies allowing individual participants to administer their data – that is, logically distribute the data
   - Distributed access implies decentralizing the service to enhance scalability and reliability – that is, physically distribute the services
5. Implement and Integrate PKI
6. Log all access calls
7. Provide a place holder for plug-in policy enforcement modules

Design Goals

- Follow Open-Closed Principle
  - Be *open* for extension, but *closed* for modification
  - In other words, be minimalistic
- Two ways to design "federated" clearinghouse
  - Include *all* features (and data) from all participating clearinghouses
    - Results in a sparse feature set (and data set)
  - Include only the *common* features (and data)
    - Results in a dense and usable set
- Clearinghouse should be forward compatible with our new GENI proposal

Registries and Data Model

User Record

Recommended (Going Forward)	Version 1.0 Impl. choice	Items	Comments	
☑	☑	ID		
☑	☐ (Optional)	Contact	Name, Email, Address, Phone.	ProtoGENI Defined
	☐	HRN	Human Readable Number	
	☒	XML-RPC Web Server URL		
☑	☑	X509 Certificate or Public key	Pem format (X509) or Base64 (Public key)	
	☒	Credential	Use ACS	
☑	☐	ACS	Access Credential Set. Placeholder.	
☑	☐	Description		

User Registry Services

Return Value	Function	Parameters	Comments
ID	Register	Contact, Description, X509/ public key	
	Update	ID, {contact or description or x509/public key}	
	Request Credentials	ID	Workflow involved. Creates ACS (credentials).
	Remove Credentials	ID	Privileged Call
ID Array	Search	Contact or Description	
User Record	Resolve	ID	

Sliver Record

Recommended	Version 1.0 Impl. choice	Items	Comments
☑	☑	ID	
	☐	HRN	Human Readable Number
	☒	XML-RPC Web Server URL	
☑	☑	Status	Overall Status
	☒	Details	Status of individual resources. See Resource Array
☑	☑	Resource Array of {Resource ID, status}	The status of resources are w.r.t. this sliver. The status of resources, when the resource IDs are resolved, describe the resource's overall status across all slivers.
☑		Description	
☑	☑	Slice ID	
☑		Expiration	Absolute timestamp

ProtoGENI Defined

Sliver Registry Services

Return Value	Function	Parameters	Comments
ID	Create Record	Resource Array, Description, Status, expiration	Privileged Call
	Bind to Slice	ID, Slice ID	Privileged Call
	Delete Record	ID	Privileged Call
	Update Status	ID, Status, {Resource ID, status } Array	Privileged Call
	Update Expirations	ID, timestamp	Privileged Call
ID Array	Search	Description or Status or Slice ID or expiration	
Sliver Record	Resolve	ID	

Slice Record

Recommended	Version 1.0 Impl. choice	Items	Comments	
☑	☑	ID		
	☐	HRN	Human Readable Number	
	☒	XML-RPC Web Server URL		ProtoGENI Defined
		X509 Certificate	Pem format	
	☒	Owner	See Administrators Array	
	☒	Administrators	See Administrators Array	
☑	☑	Status		
☑	☑	Administrators Array of {user ID, (optional) ACS, (optional) type}	The ACS here will take care of the "ticket". Type could be "owner".	
☑	☑	Sliver ID Array		
☑		Description		
☑	☑	Slice Authority ID		

Slice Registry Services

Return Value	Function	Parameters	Comments
ID	Create Record	Admin Array, Status, Sliver ID Array, Slice Authority ID, Description	Privileged Call
	Delete Record	ID	Privileged Call
	Update Status	ID, Status	Privileged Call
ID Array	Search	Description or Status or sliver id, slice authority id	
Slice Record	Resolve	ID	

Resource Record

Recommended	Version 1.0 Impl. choice	Items	Comments
☑	☑	RSpec	
☑	☑	Status	
☑	☑	ID	
☑	☐	ARS	Access Rules Set
☑	☑	Component ID	
☑	☐	Description	

ProtoGENI Defined

Resource Registry Services

Return Value	Function	Parameters	Comments
ID	Register	RSpec, Description, Status	Privileged Call
	Bind to Component	ID, Component ID	Privileged Call
	De-Register	ID	Privileged Call
	Update Status	ID, Status	Privileged Call
ID Array	Search	Description or Status or Component ID	
Resource Record	Resolve	ID	

Component Record

Recommended	Version 1.0 Impl. choice	Items	Comments
☑	☑	ID	
☑	☐	Name	
☑	☑	Component Manager ID	
☑	☑	Resource ID Array	
☑	☐	Organization Name	
☑	☐	Description	

ProtoGENI Defined

Component Registry Services

Return Value	Function	Parameters	Comments
ID	Register	Name, Component Manager ID, Resource ID Array, Organization, Description	Privileged Call
	De-Register	ID	Privileged Call
	Update	ID, {Name or Component Manager ID or Resource ID Array or Organization or Description}	Privileged Call
ID Array	Search	Description or Organization Name or component Manager ID or Resource ID	
Resource Record	Resolve	ID	

Aggregate Record

Recommended	Version 1.0 Impl. choice	Items	Comments
☑	☑	ID	
☑		Name	
☑	☑	Aggregate Manager ID	
☑	☑	Component/ Aggregate ID Array	
☑	☐	Description	

ProtoGENI Defined

Aggregate Registry Services

Return Value	Function	Parameters	Comments
ID	Register	Name, Aggregate Manager ID, Component/ Aggregate ID Array, Description	Privileged Call
	De-Register	ID	Privileged Call
	Update	ID, {Name or Aggregate Manager ID or Component/ Aggregate ID Array or Description}	Privileged Call
ID Array	Search	Description or Organization Name or component ID or aggregate ID or Aggregate Manager ID	
Resource Record	Resolve	ID	

Service (SA/CM/AM) Record

Recommended	Version 1.0 Impl. choice	Items	Comments
☑	☑	ID	
☑	☑	Type Array	An improper subset of {Slice Authority, Component Manager, Aggregate Manager}
☑	☑	Access Point	URL, for example
☑	☑	X509 Certificate or Public key	Pem format (X509) or Base64(Public key)
☑	☐	ARS	Access Rules Set

ProtoGENI Defined

Service (SA/CM/AM) Registry Services

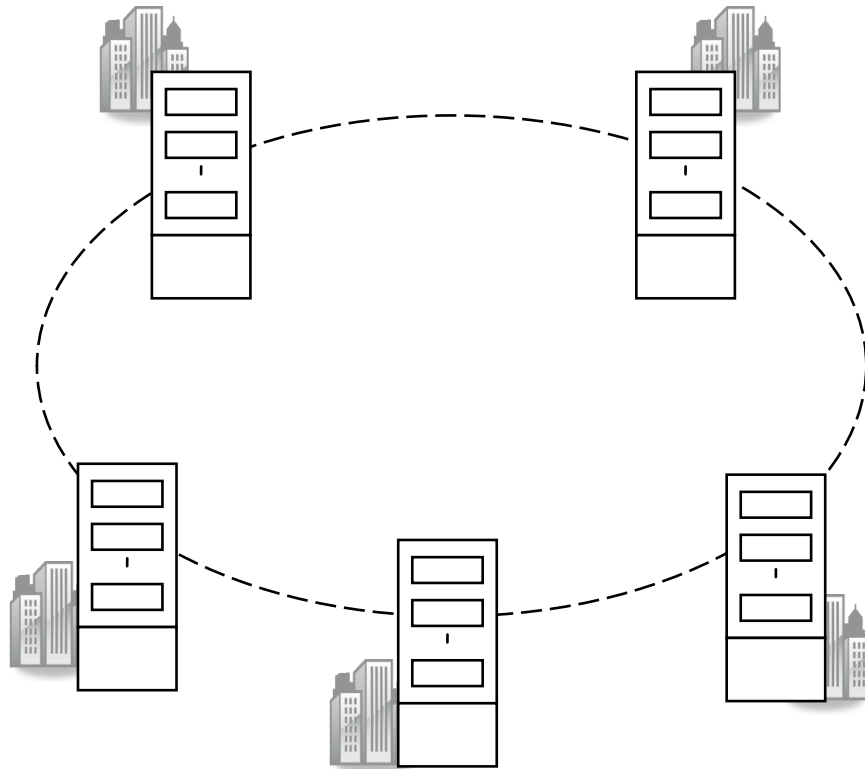| Return Value	Function	Parameters	Comments
ID	Register	Type, Access Point, x509/public key, ARS	Privileged Call
	De-Register	ID	Privileged Call
ID Array	Search	Type	
Service Record	Resolve	ID	

Authentication/Authorization Services

- Authentication Service to be implemented using the Handle System (Goal 5 – PKI)
  - Handle records store the public keys
  - Handle Protocol deals with the challenge-response for the service
- Authorization Service to be implemented using the Handle System
  - Handle records store the credential information
  - Handle Protocol supplies the credential information to the service

Clearinghouse Architecture

Individual Clearinghouse Architecture

Registries

User Registry

User ID
Public Key
ACS

Slice Registry

Slice ID

Resource Registry

Resource ID
RSpec
Status

Registries provide:
1. Registration
2. Discovery
3. Resolution

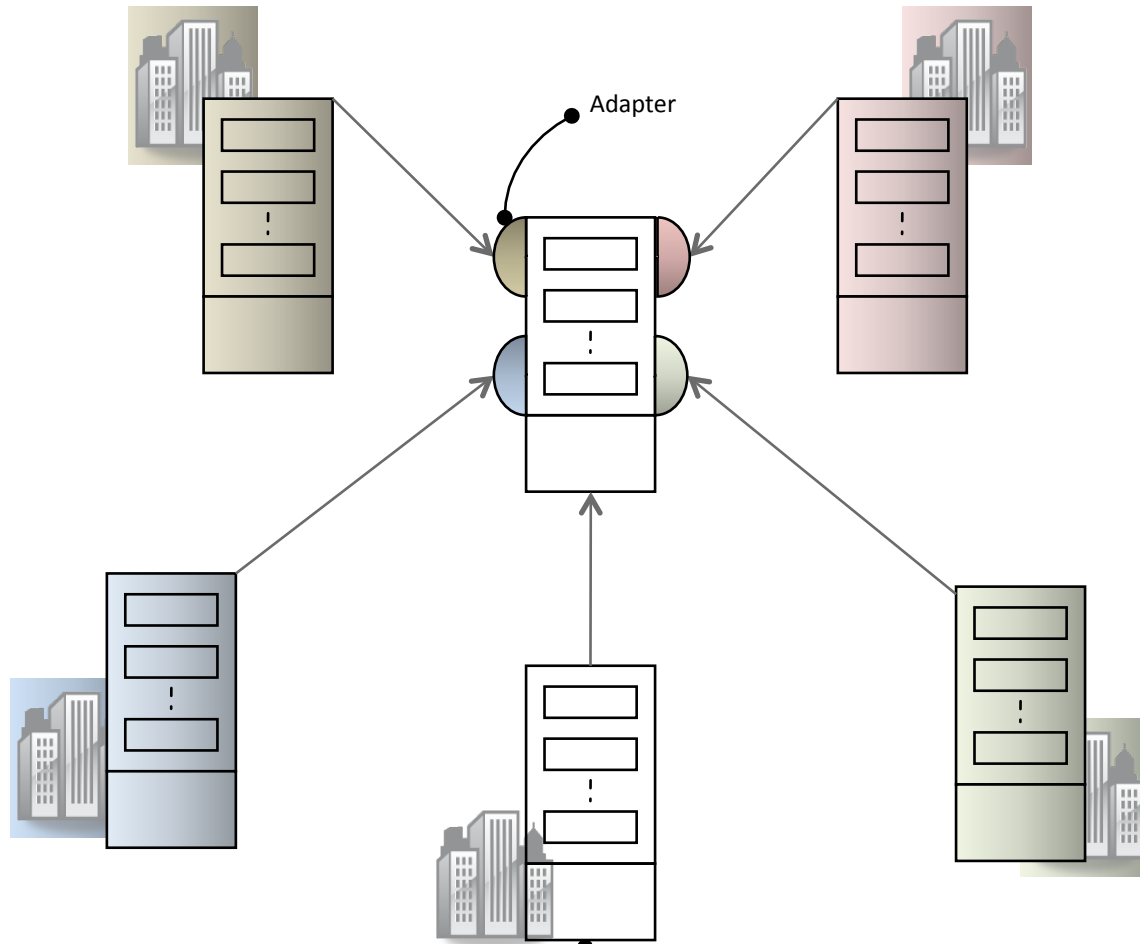Security
and
Policy
Enforcement
Sub-systems
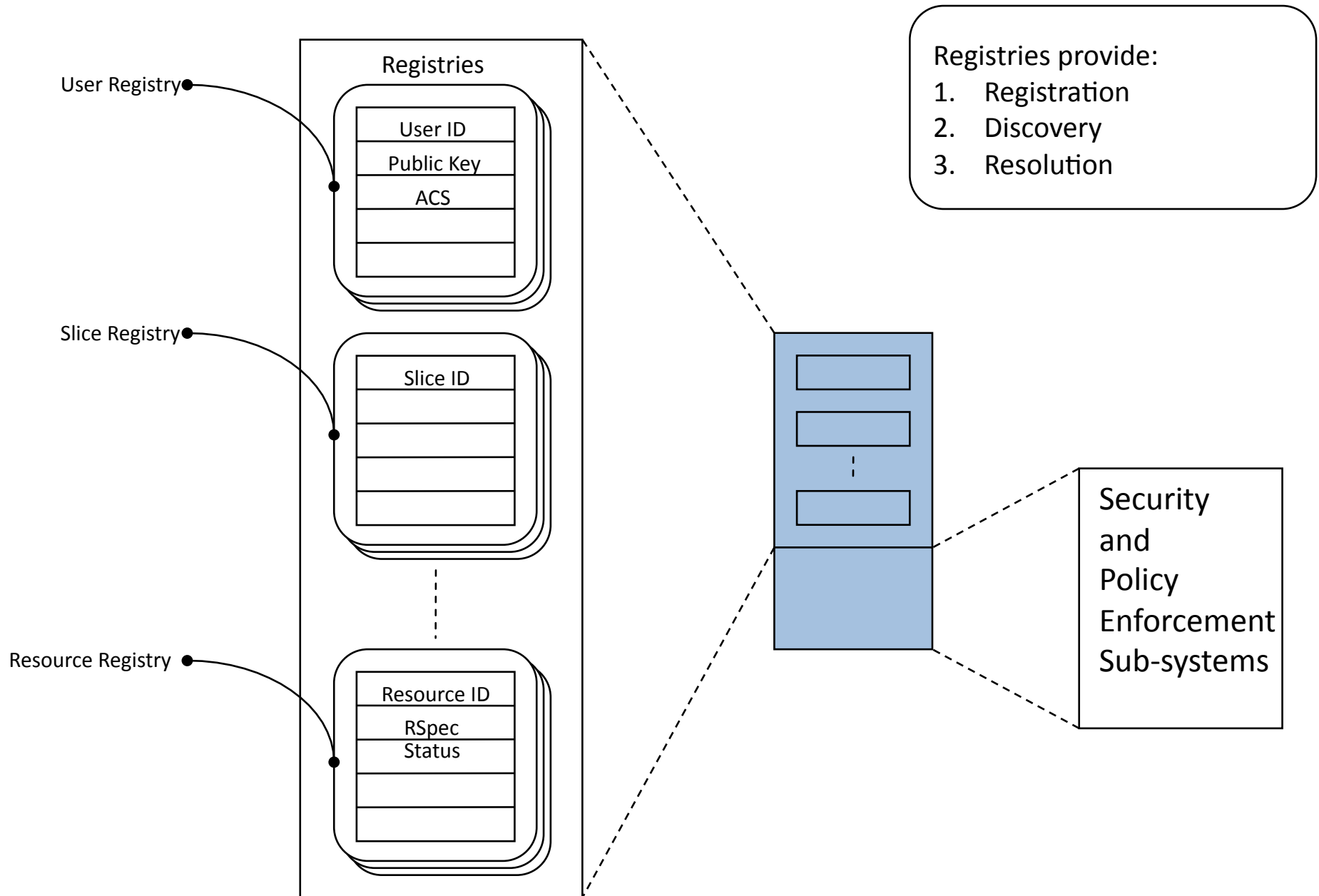
Ideal Clearinghouse Network

- Data model (and data sets) are interoperable with each other

- Identical Interface and Protocol at each clearinghouse

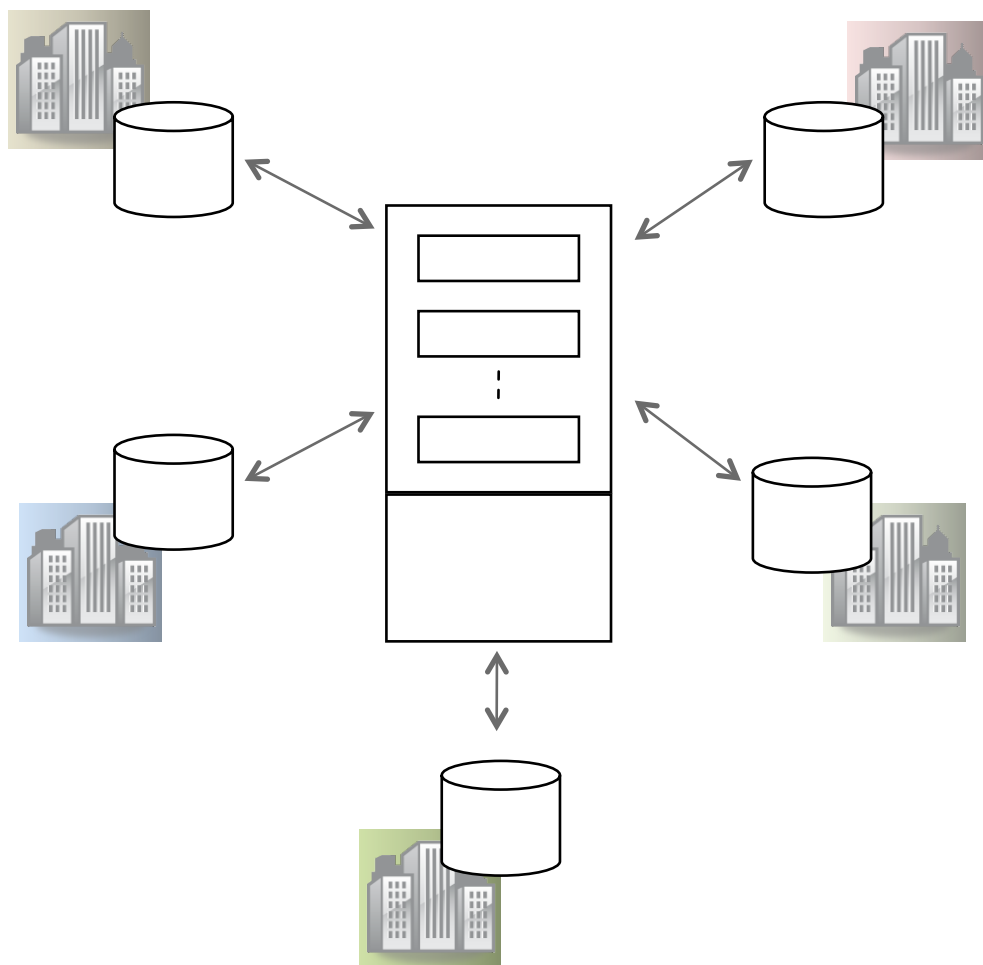- In other words, clearinghouses are logically distributed, but provide unified access to clients

GENI Clearinghouse Network

Adapter

- The mismatch among clearinghouses requires a federator aggregating data (and features) from the individual ones
- Adapters, specific to each clearinghouse, normalize the data at the federator
- The aggregating clearinghouse
  - Acts as a trusted broker between clients and control framework components (Goal 1)
  - Provides expected services (Goal 2)
  - Logs all access (Goal 6)
 - Provides a placeholder to plug-in policy enforcement modules (Goal 7)

If the proposed federator CH is deployed at the cluster level, then an adapter between the cluster-level CH and the federator CH is not required
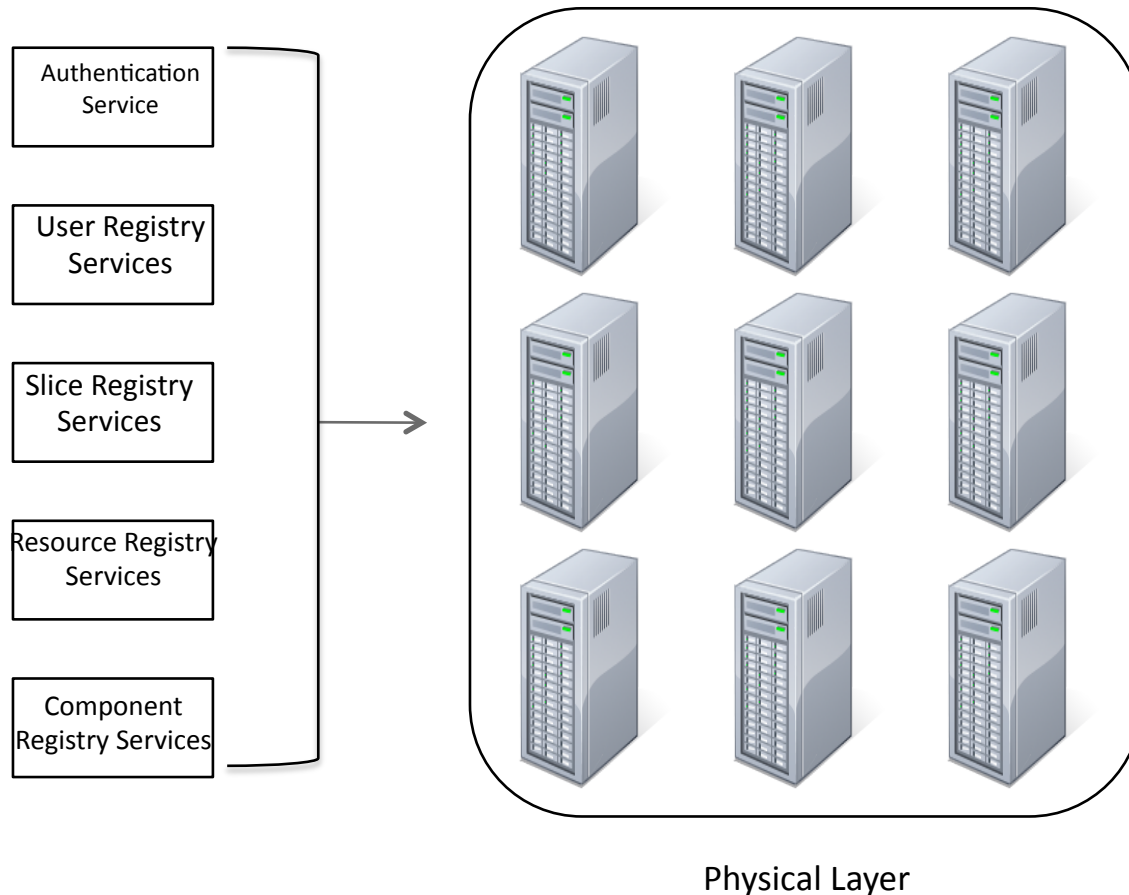
Federator Clearinghouse: View 1

- Although it appears to be centralized, the clearinghouse is logically distributed allowing
  - Individual (cluster) access to perform administration
  - Policies to be defined at individual (cluster) level
- In other words, distributed federation does not eliminate individual policy and access control (Goal 4.1)

Federator Clearinghouse: View 2

Zero-
Content
Service
Proxies
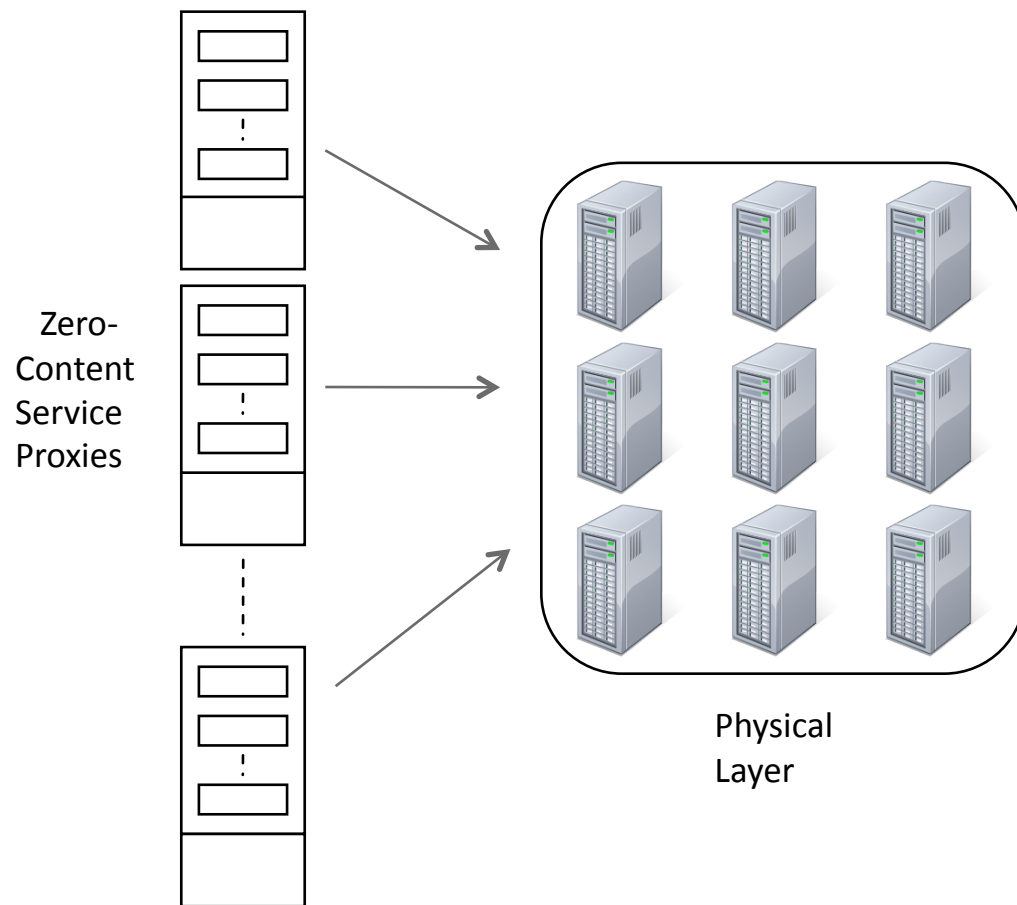
Physical
Layer

- Clearinghouse may be physically distributed with multiple (zero-content) service proxies to enable
  - Scalability, reliability, availability, etc.
- Achieves Distributed Access requirement (Goal 4.2)

Federator Clearinghouse: View 3

Authentication Service

User Registry Services

Slice Registry Services

Resource Registry Services

Component Registry Services

Physical Layer

- The services can be individually accessed and orchestrated by intermediary clients (experimental tools, for example) to provide value-added services to end users (Goal 3)