GENI Security Architecture

GEC4

Stephen Schwab, Alefiya Hussain

Miami, Florida

COBHAM

Outline

- Overview of Security Architecture Draft
  - Work in progress
- Observations About Candidate Technologies
  - Considerations for Control Framework Security Implementations

Spiral 1 Project Objective

- GENI Security Deliverable
  - GENI Spiral Security Design Reports – Develop… a series of pragmatic near-term security design documentation used to guide and coordinate GENI prototyping teams regarding the adoption and incorporation of key security properties into the evolving D&P implementations.
- SPARTA not tasked to build, implement, integrate security functions in spiral 1

Overview of Security Architecture

Draft

- Threat model
  - – Researchers Authenticated/Authorized to use available resources within a control framework
  - – External attacks, accidental experiments, slice isolation, …
- Trust model
  - – Explicit trust assertions
    - Multi-way trust between researchers ←→ resource owners
  - – Local decision making by distributed components

Security Architecture “Major Points”

- Explicit Trust, Least Privilege
- Revocation
- Auditability and Accountability
  - All of the above address central security properties of GENI Infrastructure

- Scalability, Autonomy, Usability, Performance
  - All 1st order issues that take into consideration the anticipated usage model and evolution of GENI

Security Architecture Draft

- Mechanisms to be addressed in Spiral 1
  - Identity
  - Authentication
  - Authorization
  - Access Control
- Description and Analysis of how Control Frameworks are pursuing their own paths to security in Spiral 1

COBHAM

Security Architecture Draft

- Spiral 1 Action Items list
  - Roots of Trust, POCs and operational information
  - Audits, Source Code reviews
  - More discussion of issues in OMIS WG tomorrow
- Candidate Technical Mechanism
  - Attribute Based Access Control
- Comment and discussion invited on posted draft
  - groups.geni.net/geni/attachments/wiki/GENISecurity/GENI-SEC-ARCH-0.4.{doc,pdf}

Observations on Spiral 1

- Observations About Candidate Technologies

- Well-known, deployed at scale
  - HTTPS to centralized web site, Anti-virus scanners, PGP
- Well-known, various stages of deployment
  - DNSSEC, X.509 PKIs, …
- Mature research prototypes, not previously deployed at scale
  - ABAC, SHARP, …

COBHAM

Security for GENI Spiral 1

- Essential building block for integration within each control framework
- Tenets of Architecture
  - Separation of authenticated identity and authorizations
  - Explicit credentials for authorization
  - Flexibility and scale
- Technologies
  - What exists, how it might be adapted for GENI
  - Shibboleth, Attribute Based Access Control, …

Separation of ID and Auth.

- Identity represents a unique entity in GENI ecosystem
  - May have different roles in different GENI control frameworks/clusters, that is, operator vs. researcher
  - lightweight
- Authorizations are built from *primitive* statements about identities that trusted *authorities* are willing to certify
  - Anyone can act as an authority
  - Can delegate rights (e.g. specific privileges)

Authentication

- Authenticate the principal who is acting within the GENI suite
  - Utilize a public key
- May check with registry about status
  - Active with current public key
  - Negative with Certificate Revocation List

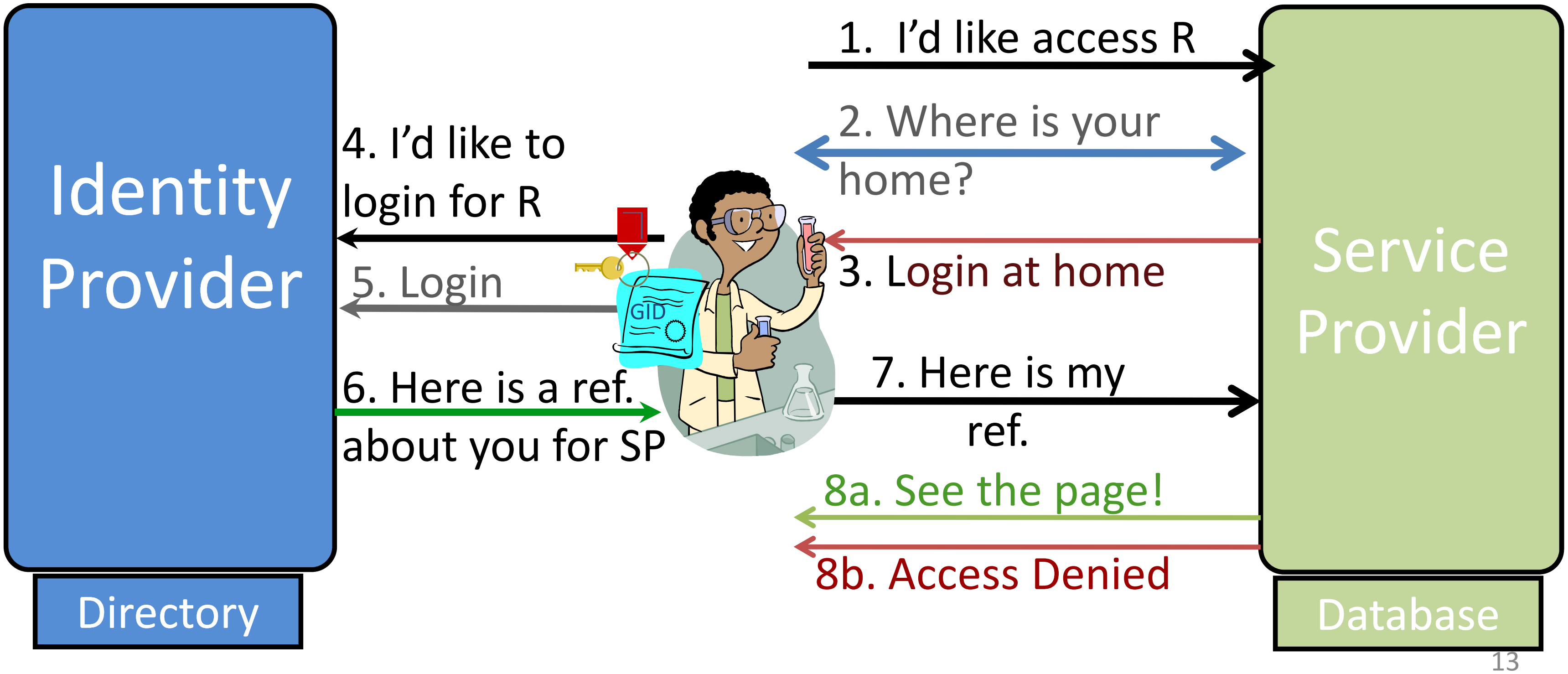
Trust, Assertions, Reasoning

- Which entities are trusted principals (authenticated identities)?
- Assertions about entities (attributes)
  - What can be expressed? In what syntax or language? Is it extensible or fixed?
- Making inferences that lead to authorization (reasoning)
  - What rules are used to combine attributes?
  - Are these implicit in the reasoning algorithm or explicit?

- *From a Security Architecture viewpoint, do we need to lock ourselves in* now*?* Spiral 2 or spiral 3?

Shibboleth

- Single sign-on, tied to the web browser/server model
- Services no longer manage user accounts & personal data stores
- Home org controls privacy



Identity Provider

Directory

1. I'd like access R

2. Where is your home?

3. Login at home

4. I'd like to login for R

5. Login

6. Here is a ref. about you for SP

7. Here is my ref.

8a. See the page!

8b. Access Denied

Service Provider

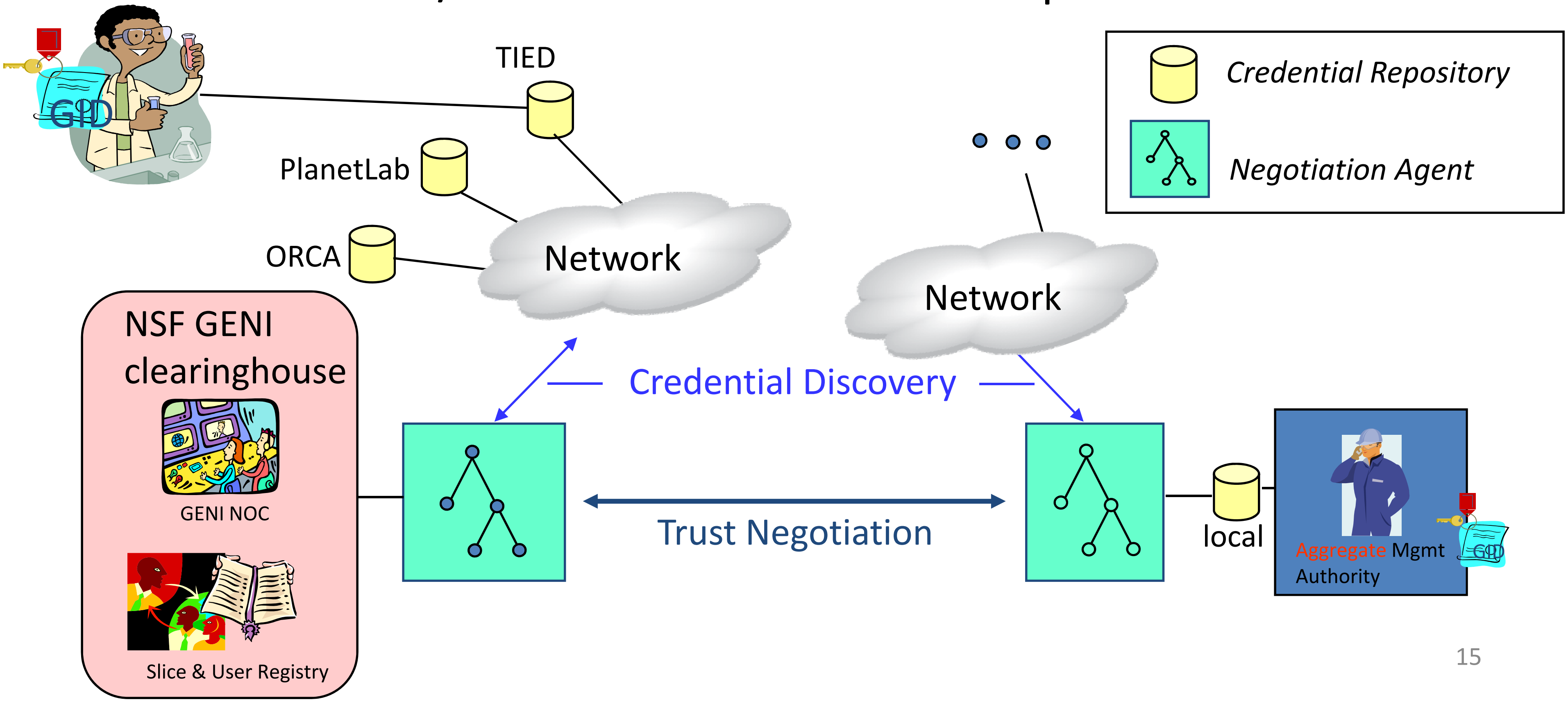
Database

Shibboleth Terminology

- Identity Provider supplies assertions
  - Attribute Authority (AA): Acquires user attributes and encodes them for transport
- Service Provider receives assertions and protects resources
  - Assertion Consumer Service (ACS): Receives assertion, processes it, passes user along
- The reference is essentially an attribute, a name/value pair that describes the user
- User authentication and attribute information wrapped as SAML (Security Assertion Markup Language) for transport
- A trust structure to help large communities of IdP and SP to interoperate

Attribute-based Access Control

- Chains of digitally signed credentials for authorization
- Credential storage is distributed
- Attributes/Roles define access control permissions



Attributes Defined

- Subject Attributes
  - Associated with a subject (user, application, process) that defines the identity and characteristics of the subject
  - E.g. identifier, job title, role (PI, faculty,admin)
- Resource Attributes
  - Associated with a resource (service, system function, or data)
  - E.g. terminate, preferred
- Environment Attributes
  - Describes the operational, technical, or situational environment or context in which the access occurs
  - E.g. current time, lifetime, wireless, BER

ABAC Example

SA permits complete slice termination by an operator hosting the sliver/component at their local site

SASliceA.shutdown ← MASliverA.creator

MASliverA.creator ← LocalSite.faculty

LocalSite.faculty ← Dean.faculty

Dean.faculty ← Ted

Flexible Credential Definitions

- SASliceA.shutdown ← SA.admin.faculty

  SA responsible for SliceA says that LocalMA entity has an attribute *admin*, and the LocalMA says that an entity X has an attribute *faculty*, then SASliceA says that X now has attribute *shutdown*

- SASliceA.shutdown ← creator and admin

  Any entity that has the attributes *creator* and *admin* is authorized to perform a SliceA *shutdown*

Control Frameworks – Spiral 1

- Examining Security Mechanisms in the Control Frameworks
  - PlanetLab
  - ProtoGENI
  - ORCA
  - ORBIT
  - TIED

Backup

PlanetLab Solution

Protocol between researcher and GENI entity (MA/SA/CH)

- exchange and authenticate GID

- exchange and authenticate credentials

Terms

- UUID, a unique id for each object within the system
- DN, corresponds to a chain of authorities that vouch for the object planetlab.princeton.codeen
- GID = <UUID,public_key,DN,type>, a certificate, DN indicates signing authorities, type associated with object
- Slice Credential = <pubkey, DN, type>
- Ticket = <pubkey,rspec,lifetime>

ORCA Solution

Protocols between users and GENI entities

- Principals, connect with the Broker, Domain Authorities and Service Managers, exchange and authenticate

- Service Managers (Experiment Control Tools) are used by the researchers to setup and authorize slices

Terms

- Broker=Clearinghouse, trust management
- Domain Authorities=Aggregate Managers, control Components, e.g., an array of hosts at a site, or a network domain
- Service Managers = Slice Controller
- Identity Providers, which vouch for Principals
- Lease contract=ticket

ProtoGENI Solution

Protocols

- Exchange of credentials/tickets for authorization

- Credentials certified by signing with priv key by authority chain up to the root authority

- PKI is used to authenticate principals and provides keys to sign and verify credentials

Terms

- Clearinghouse = registry for Principal/slice/aggregate/services
- Slice Authority = Emulab site services
- Aggregate Manager = all hosts and resources within Emulab
- GID = <UUID, GNAME>
- WSDL, XML_RPC, SSL for messages and authentication
- Credentials signed by SA to give value

ORBIT Solution

Protocols

- Delegates approval of user accounts to parent institution
- Resource conflicts resolved using a reservation calendar system, time-based single user access
- PKI for authentication

Terms

OIDL, a domain specific language to request resources

TIED

Protocols

- Based on single-Emulab model, project-based access control

- Federation architecture - three level model:

  - Users, projects, testbeds have global names
  - Federants honor accesses based proof of name, attested facts (evaluated wrt name) and local information bound to name
  - Once accepted, federants assign accepted sub-experiments to local projects for resource control

Terms

Identity

- Unique, assigned to each entity in GENI
  - Users, components, slices
  - Examples: Pub-priv key pair, GID, UUID

- Identities vs. names

Access Control

Defn: mechanism to reach a yes-no decision with respect to granting access to a resource.

Traditional methods do not scale and are not flexible

Identity-based approach: Each resource has an *access control list* that indicates users that are authorized to access it.

Capability-based approach, Each user has a resource list/*capability* that is reviewed for access control

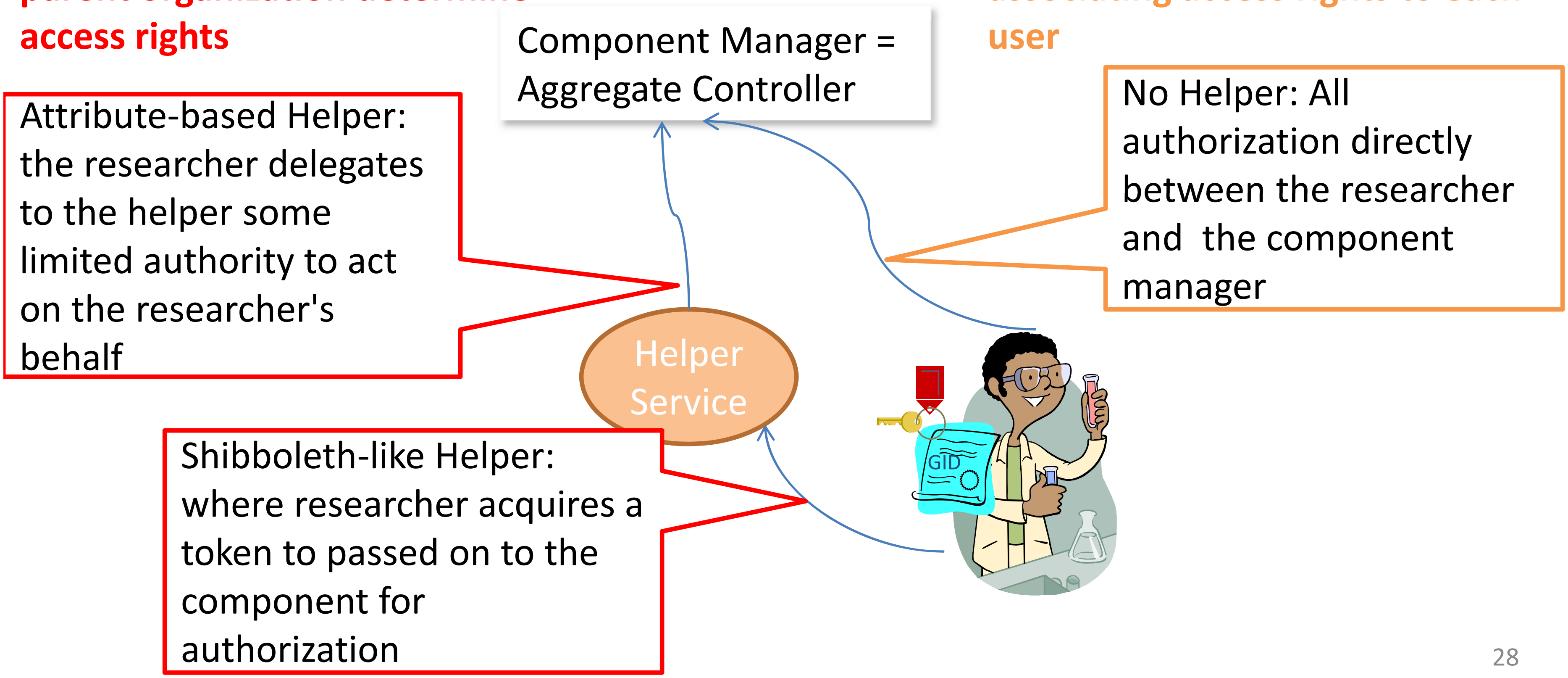
	Resource1	Resource 2	Resource3
user1	X	X	
user2		X	X
user3	X	X	

Authorization

Defn: process of allowing access to resources only to those permitted to use them

Attributes/Role in researchers parent organization determine access rights

Requires maintain databases associating access rights to each user



Component Manager = Aggregate Controller

Attribute-based Helper: the researcher delegates to the helper some limited authority to act on the researcher's behalf

No Helper: All authorization directly between the researcher and the component manager

Shibboleth-like Helper: where researcher acquires a token to passed on to the component for authorization

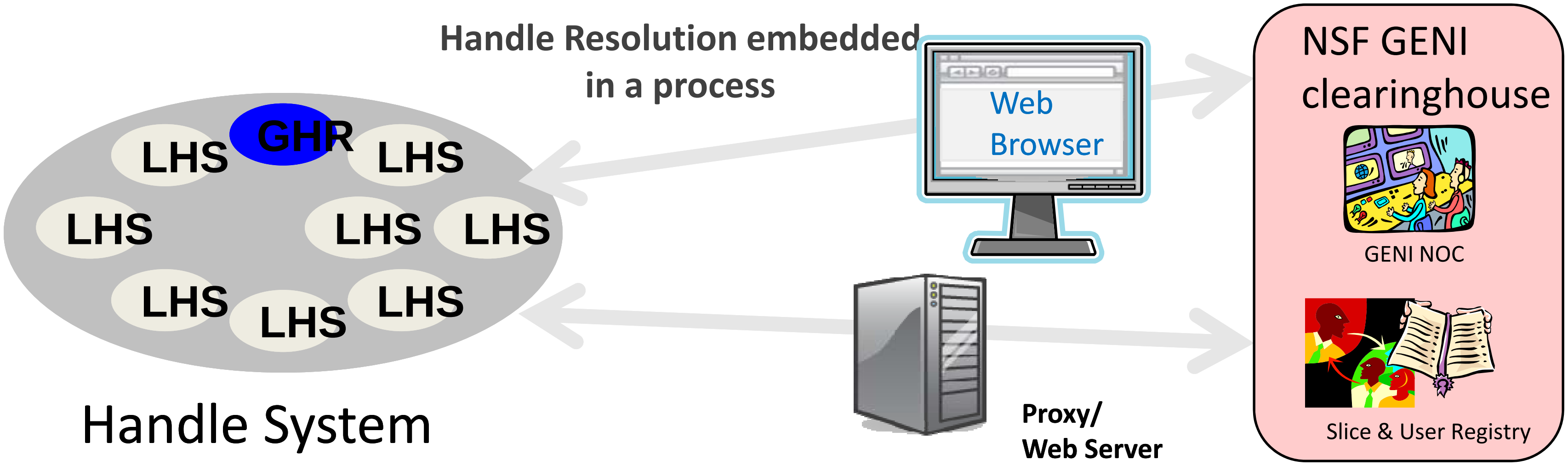
CNRI's DOA

Digital Object Architecture

- Handle System
  - scalable identifier resolution system for digital objects
- DO Data Model and Protocol
  - Interface to the information management and storage systems
  - Strong authentication and encryption technologies
- DO Repository
  - Portal into multiple info and storage systems
- DO Registry
  - Composable services and search facility across multiple DO Repositories

Handle System

- Provides ID resolution
- Logically centralized, but physically and organizationally distributed, highly scalable
- Association of multiple typed values to id
  Ex: IP address, public key, HRN
- Secure resolution with PKI as an option



ABAC Policy Definitions

- SA_k ($1 \leq k \leq K$), RA_m ($1 \leq m \leq M$), and EA_n ($1 \leq n \leq N$) are the pre-defined attributes and *ATTR(s)*, *ATTR(r)*, and *ATTR(e)* are attribute assignments for subjects, resources, and environments where,

$$ATTR(s) \subseteq SA_1 \times SA_2 \times \ldots \times SA_K$$

$$ATTR(r) \subseteq RA_1 \times RA_2 \times \ldots \times RA_M$$

$$ATTR(e) \subseteq EA_1 \times EA_2 \times \ldots \times EA_N$$

- *Credential discovery* decides on whether a subject *s* can access a resource *r* in a particular environment *e*