# GENI and Federated Identity, Authorization and Resource Management

## LSN MAGIC Meeting – January 8, 2014

**Marshall Brinn**
**GENI Program Office**
**www.geni.net**

Sponsored by the National Science Foundation

# Outline

- Introduction : GENI Federation Concepts
- GENI Identity and Authentication
- GENI Policy and Authorization
- GENI Resource Management
- Recent Developments
- Next Steps

# Federation is essentially a human activity

## Resource Owners

Managers or owners of equipment that they want to share, provided the resources can be…

- Protected from misuse, overuse
- Prioritized as necessary
- Monitored for forensics

## Federations

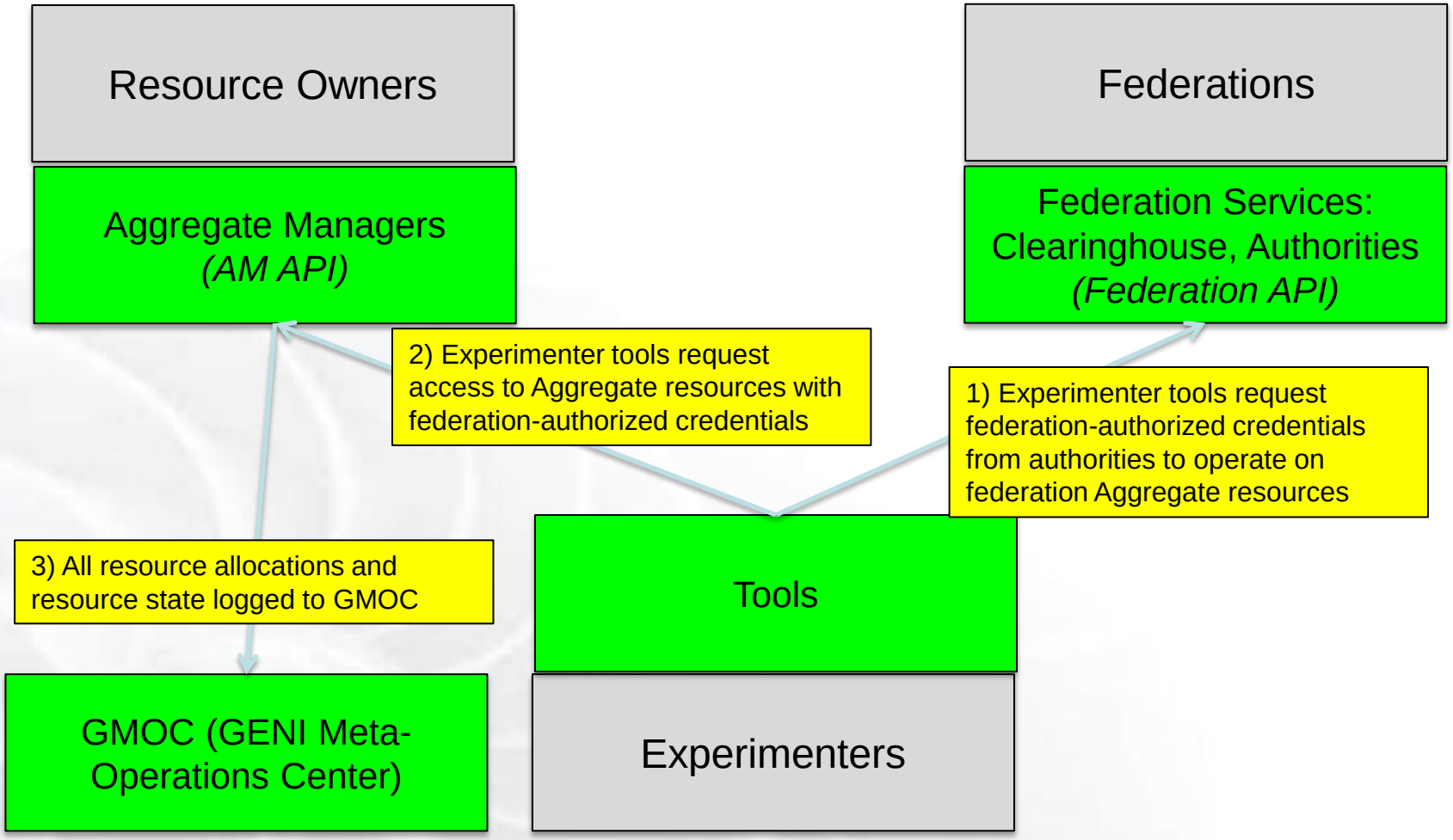
Groups of people who facilitate the agreements between Resource Owners and Experimenters to enable them to share resources confidently

## Experimenters

Researchers who want to construct a configuration from a variety of resources to perform their experimentation, provided the resources can be…

- Reliable (available, recoverable)
- Isolated
- Monitored for performance

# GENI Provides S/W Services that represent the interests of these human participants




These interactions can be trusted to enforce federation agreements with a strong ***common identity and policy framework***.

# GENI Identity and Authentication

- GENI recognizes two classes of identity:
  - GENI-internal: between GENI services (Aggregates, Federation Services) we authenticate service invocations via PKI (public/private key-pairs and certificates)
  - GENI-external: For federating with other *trusted* identity providers, we provide tools that bridge external identities to GENI-internal credentials

# GENI & InCommon

- GENI Portal is an InCommon Research and Scholarship (R&S) Category Service Provider
  - Automatic access for users of InCommon Identity Providers that implement the R&S category
  - More info: InCommon web, “Identity Providers that Support R and S”
- User identity supplemented with GENI-managed attributes (e.g., “Project Lead” privilege)

# Bridging InCommon and GENI

The GENI Portal is a member of both federations

GENI Federation

Clearinghouse

svc svc svc svc svc svc

GENI Portal

Agg Agg Agg Agg

InCommon Federation

The GENI Portal fulfills obligations to each federation

# Benefits of federated identity

- InCommon Users
  - Users simply arrive and have immediate access
  - Dramatically reduced management effort for GENI
    - No password management, no updating attributes, etc.
    - Unsolicited comment from new project lead: “BTW, linking in the accounts with our university's accounts is awesome!”
- Non-InCommon Users
  - GENI manages its own IdP and can add new accounts
  - Same as InCommon users to GENI Portal
  - After about fourteen months of operation, GENI Portal now has 1071 registered users – approximately 60% from InCommon, 40% using GENI IdP.
  - Other federation example: GENI is currently federated with CAFe (Brazil)

# GENI Federation: Trust and Policy

GENI Federation is a set of aggregates and authorities that chose to collaborate for a common purpose

- This federated collaboration is facilitated by establishing ***common trust roots***
  - "I accept credentials signed by these entities."
- A federation also establishes ***common policies*** for resource allocation
  - Authorities provide credentials based on these common policies
  - Aggregates use these credentials as inputs to their policy-based allocation authorization decisions, which may include additional aggregate-internal (local) policy requirements

# Authorization and Accountability in GENI

- GENI seeks to assure that all actions on resources are:
  - **Authorized**: Actions may only be taken by a given user if permitted by policy
    - Both local and federation policies
  - **Accountable**: Actions are attributed to the responsible user
    - Supporting granular reports and controls of resource usage
    - Allowing for forensics and responsibility in case of inappropriate resource usage (intentional or unintentional)

The GENI Architecture is designed to provide such assurances

# Policy Representations in GENI: Current

GENI supports different types of Authorization policy forms

- **RBAC** ("Role-based" Access Control): Provides a fixed set of permissions to a given user to a given resource (e.g. slice) – SFA slice credential
  - "X can create or delete slivers on slice Y"
- **ABAC** ("Attribute-based" Access Control): Provides a dynamic set of permissions based matching attributes of user and policy requirements.
  - Policy statements and assertions about user attributes have distinct explicit external representations which are composed dynamically at policy decision points
  - E.g. Policies
    - "Anyone who is a 'lead' of a slice can add members to that slice"
    - "Anyone that is a TA in a course can administer a project of that course"
  - E.g. Attribute Assertions
    - "Joe is the lead of slice 'TEST2014'"
    - "Mary is a TA of course 'CS101'"

# Policy Representations in GENI

Some policy statements require greater expressivity and computation than pure RBAC/ABAC logics can provide

- **Quantity-based** : Statements about quotas to projects, slices, individuals or groups
  - "A member of this project can have up to 4 VMs."
  - "No user can consume more than 60% of the bandwidth on a particular connection."
- **Time-based**: Statements that change with time
  - "Experimenters outside of this university can have 50% of our VM's during finals week and 75% otherwise"

Implementation may require straightforward helper code.

# GENI Authorization and Accountability: Speaks-for and Speaks-as

- GENI users need tools to speak the Authority and AM (Aggregate Manager) APIs on their behalf
  - The simple-minded approach is to give tools the user's cert/private-key and allow the tool to "speak as" the user
  - A bad idea for two reasons:
    - Key security: Passing private keys is very bad practice
    - Accountability: The tool's role in transactions is not visible to aggregates and GMOC
- GENI "speaks for" mechanism
  - A user signs a statement authorizing a given tool to act on the user's behalf in some context (e.g. a slice, a time period)
  - The tool "speaks as" itself (i.e uses its own cert/key) to authorities and aggregates
  - The authorities and aggregates can authorize actions based on the user's credentials but account the action to the tool
  - The user's private key is never transmitted.

# GENI Resource Management

- The lifecycle of an experimenter working with GENI is a continued application of this pattern:
  - **Authentication**: Identification to Federation Services and Aggregate Managers using PKI credentials signed by a trusted root
  - **Authorization**: Receive appropriate rights/credentials to perform particular resource-related actions (allocate, renew, reconfigure, release, describe, etc.)
  - **Allocation:** Dedication and configuring of requested resources (pending availability and authorization)
  - **Accountability**: Aggregate Managers report what resource allocation requests have been made (success or failure) for federation-wide reporting, monitoring, forensics

# GENI Resource Management [2]

- This pattern is particularly useful, because in GENI (nearly) EVERYTHING a researcher wants to allocate, configure and use is a resource managed by an aggregate manager
  - Bare-metal and virtual machines
  - Storage (disks, databases)
  - Services (storage, web servers, monitoring/forensics)
  - Cross-domain network connections (“stitches”)
    - Allocation and configuring of common VLAN-tags
  - Flow-space and network nodes/links for allocation of Software-Definable Networks

# Recent Developments

- **Federation API** : Recent collaboration between Fed4Fire (EU), GENI, Emulab for standard federation (Clearinghouse, Authority) and resource interfaces
  - Federation API v1 implemented and running
  - Federation API v2 ratified and upgrades underway
  - Resource API v1 (based on GENI AM API) standards discussions underway

# Recent Developments [2]

- **Virtual Organizations**: Recent discussions with Jim Bottoms of Clemson and IDM WG about applying GENI Project/Membership concepts to support ad hoc VO's.
- **Cross-Federation Operations**: Discussions underway to discuss cross-domain monitoring, forensics, "manager of manager" with limited control/visibility into individual federations

# Identity & Access Policy in GENI: Next Steps

- GENI does not want to be in the identity business
  - We plan to work with campus and test-bedresource provider community to help identify shared needs.
  - GENI is ready to be an early service provider adopter of relevant new identity capabilities.
- GENI is actively innovating in the policy space.
  - Architecture separating aggregates, tools, and people is central to GENI.
  - ABAC-based policy statements and distributed enforcement provides policy clarity and proof-supported decision-making.
  - “Speaks as” and “speaks for” delegation for accountability


**Marshall Brinn**
**GENI Project Office**
**January 8, 2014**
**mbrinn@bbn.com**
**www.geni.net**