Identity Management and Attributes in GENI

Proposed Implementation

Tom Mitchell

GEC 10

March 15, 2011

Sponsored by the National Science Foundation

Proposal

- Add external identity providers to GENI
- GPO should build an InCommon compatible GENI portal/slice authority
- Agree on an initial set of required identity attributes

GENI Portal

- Create a GENI web portal
  - For new GENI experimenters
  - Authenticate using their own institutional accounts
  - Shibboleth Service Provider
  - Federated with InCommon
- Similar to TeraGrid use case
  - See background reading

GENI Portal Overview

GENI Portal

Institutional Identity Provider

John Smith
faculty@example.edu
john@cs.example.edu

Primary Identity Information

Net Research Group
GEC Demo Group

NRG slice A
NRG slice B
GDG slice 7

GENI Group Attributes

GENI Attributes

Additional Identity Information

GENI Portal: Attributes

- Accept experimenter attributes from institutional IdPs
- Ask experimenters to self-assert missing attributes
- Administrators verify/validate self-asserted attributes
- Administrators approve (or deny) account requests

- The GENI Portal acts as a registry of accounts
  - Stores self-asserted attributes
  - Maintains GENI-specific information (slices, groups, etc.)
  - Permits associating GENI account with other identities (eg. change of institution)

GENI Portal: Bridge to GENI

- Near Term
  - Portal generates X.509 certificate for experimenter
  - Portal acts as a GENI Slice Authority
  - Portal generates slice credential for experimenter
  - Slice credential allows resource manipulation at GENI aggregates via GENI AM API
- Future
  - Accept attributes and identities from more sources
  - Portal can generate attribute assertions
    - eg. ABAC or SAML
  - Depends on Authorization discussion

Getting Attributes to GENI

- Identity providers decide what attributes to send to service providers like GENI
- InCommon IdPs may provide all, some or no GENI required attributes
  - Expected to be highly variable at first
  - Some will never provide all due to privacy concerns
- Bridge the gap by allowing experimenters to self-assert attributes.
  - Administrators verify/validate
- Other Shibboleth tools can also provide attributes
  - Grouper, CoManage

Desirable Experimenter Attributes

Attribute	InCommon Attribute	Example
Full Name	givenName, sn	John Smith
Institution	entityID + metadata	Example University
Institutional Affiliation	eduPersonScopedAffiliation	member@example.edu, faculty@example.edu
Email Address	mail	jsmith@cs.example.edu
Phone Number	telephoneNumber	212-555-1234

- We think GENI needs to know:
  - Who an experimenter is
  - Where they are from
  - How to contact them when something goes wrong

Pros

- Leverage external identity management
  - Let the experts handle it, stand on their shoulders
  - Access institutionally asserted and maintained attributes (email address, class enrollment, etc.)
  - Authoritative statement of affiliation
- One of many types of federated identity
  - Other Shibboleth-based federations, OpenID (Google, Yahoo, etc.), Facebook Connect, etc.
- Lower the barrier to entry for members of InCommon institutions
  - About 200 Higher Education Institutions
- Minimal disruption to existing aggregates
  - Add GENI portal as a trusted slice authority

Cons

- Still requires storing experimenter attributes
- Still requires administrative approval
- Multi-step process to gain access to GENI
- Requires identifiable attributes – no anonymous access

Draft Schedule

- By GEC 11
  - GPO will develop a prototype GENI Portal
  - GENI portal to become an InCommon Service Provider
  - Work with a few member institutions to provide desired attributes
  - Issue certificates and credentials based on InCommon identities
  - Federate with a few GENI aggregates
- By GEC 12
  - Pending Authorization discussion, pass attributes to aggregates for richer authorization decisions

Shibboleth Tools

- CILogon
  - Generates an X.509 Certificate based on an identity
  - Already an InCommon service Provider
  - Does not provide access to most attributes
- COmanage
  - Collaborative Organization Management Tool
  - Allows privileged individuals to manage group memberships
  - Works like secondary identity provider

Conclusion

- A GENI Portal is straightforward
  - No obvious technical hurdles
  - Others (TeraGrid) have done similar things
- A GENI Portal can be backward and forward compatible
- GENI needs a small number of attributes
- Many more attributes may be available to GENI

Proposal

- Add external identity providers to GENI
- GPO should build an InCommon compatible GENI portal/slice authority
- Agree on an initial set of required identity attributes

Agenda

- Introduction - Tom Mitchell (5 mins)
- IdM Principles and key issues - Ken Klingenstein (20 mins)
- Proposed implementation - Tom Mitchell (15 mins)
- Invited discussion - Rob Ricci (10 mins)
- Invited discussion - Jeff Chase (10 mins)
- Open Discussion - All (20 mins)
- Summary and Wrap Up - Tom Mitchell (10 mins)