Managing Security Policies for OGF NSI Authorization

Stephen Schwab, John Wroclawski, Ted Faber
{schwab,jtw,faber}@isi.edu

USC Information Sciences Institute

March 26, 2015

Outline

Motivation: Security Policy Issues for Federated* Cyber Infrastructure

Technology: Attribute Based Access Control

Experience: DETER and GENI

Current Focus: User Interface Tools and Community-centric Policy Metaphors

Properties of Federated Cyberinfrastructure

Flexible

dynamic set of participating organizations and facilities

Sustainable

evolves over various timescales

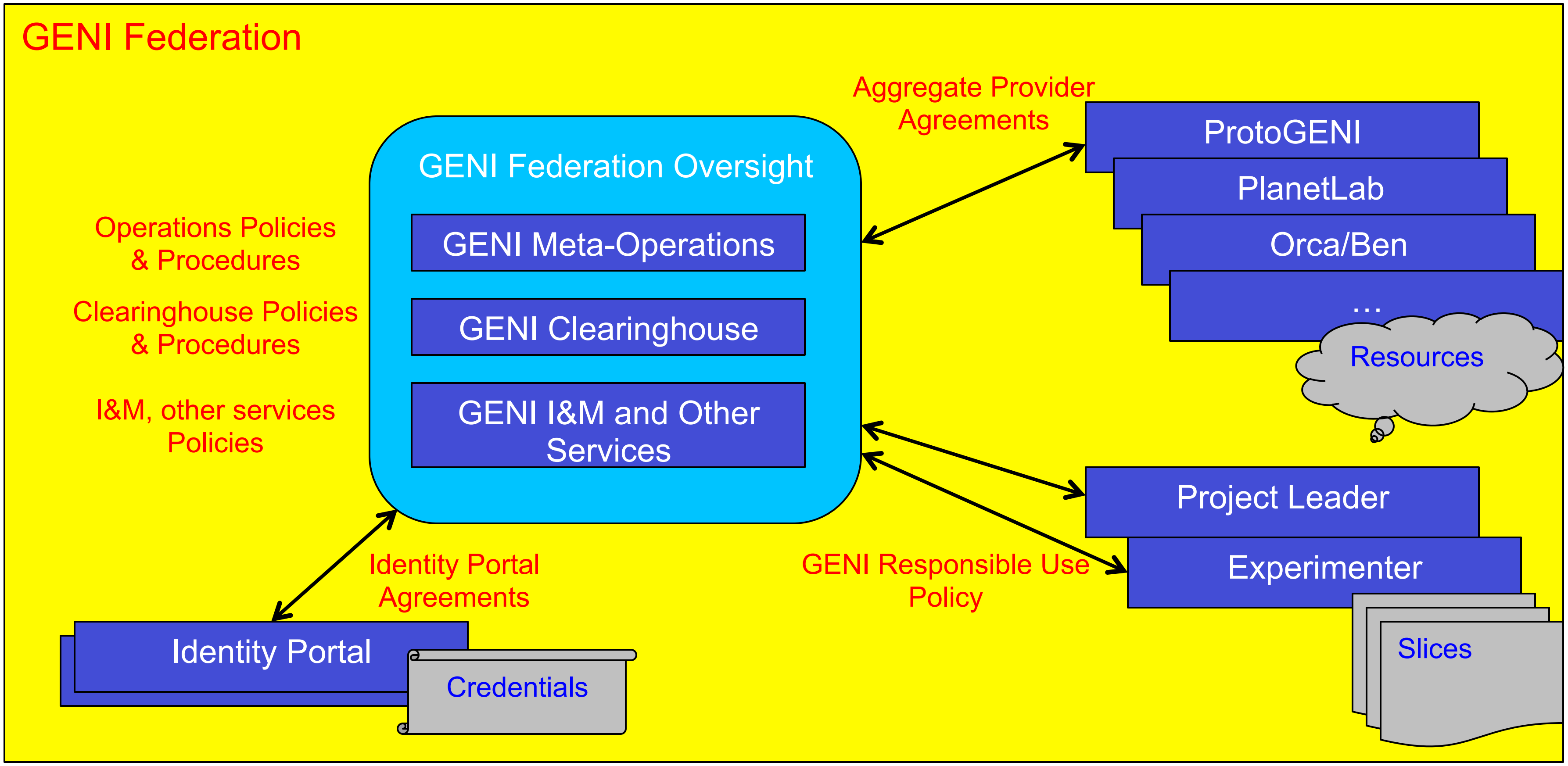
Brings resources

of both similar and disparate types…

together for ephemeral duration…

to accomplish a specific function or purpose.

What do we mean by Federated Cyberinfrastructure?



GENI Federation

Aggregate Provider Agreements

GENI Federation Oversight

GENI Meta-Operations

GENI Clearinghouse

GENI I&M and Other Services

Operations Policies & Procedures

Clearinghouse Policies & Procedures

I&M, other services Policies

ProtoGENI

PlanetLab

Orca/Ben

…

Resources

Project Leader

Experimenter

Slices

Identity Portal Agreements

GENI Responsible Use Policy

Identity Portal

Credentials

What security problems are we solving?

1. Policy Structure and Vocabulary

- Ability to Express Interesting Policies
  - Basic Constructs: Hierarchy, Roles, Delegation, Groups, etc.
- Reflections of Organizational Structure
  - Mirrors the organizational complexities and interactions of inherent complexity arising in large-scale scientific endeavors and projects
- Vocabulary
  - Terminology defined by and meaningful in the context of individuals, projects, research communities and institutions
  - Different vocabularies or extensions used by different sub-communities

What security problems are we solving?

2. Federated Facilities retain Local Control

Definition: *Federation – an organization or group within which smaller divisions have some degree of internal autonomy.*

Policy rules are defined locally

- Policies may inherit, share, reuse or adapt global rules
- Federations may require compliance with some aspects of their overall federation policy

What security problems are we solving?

3. Auditability and Formal Verification

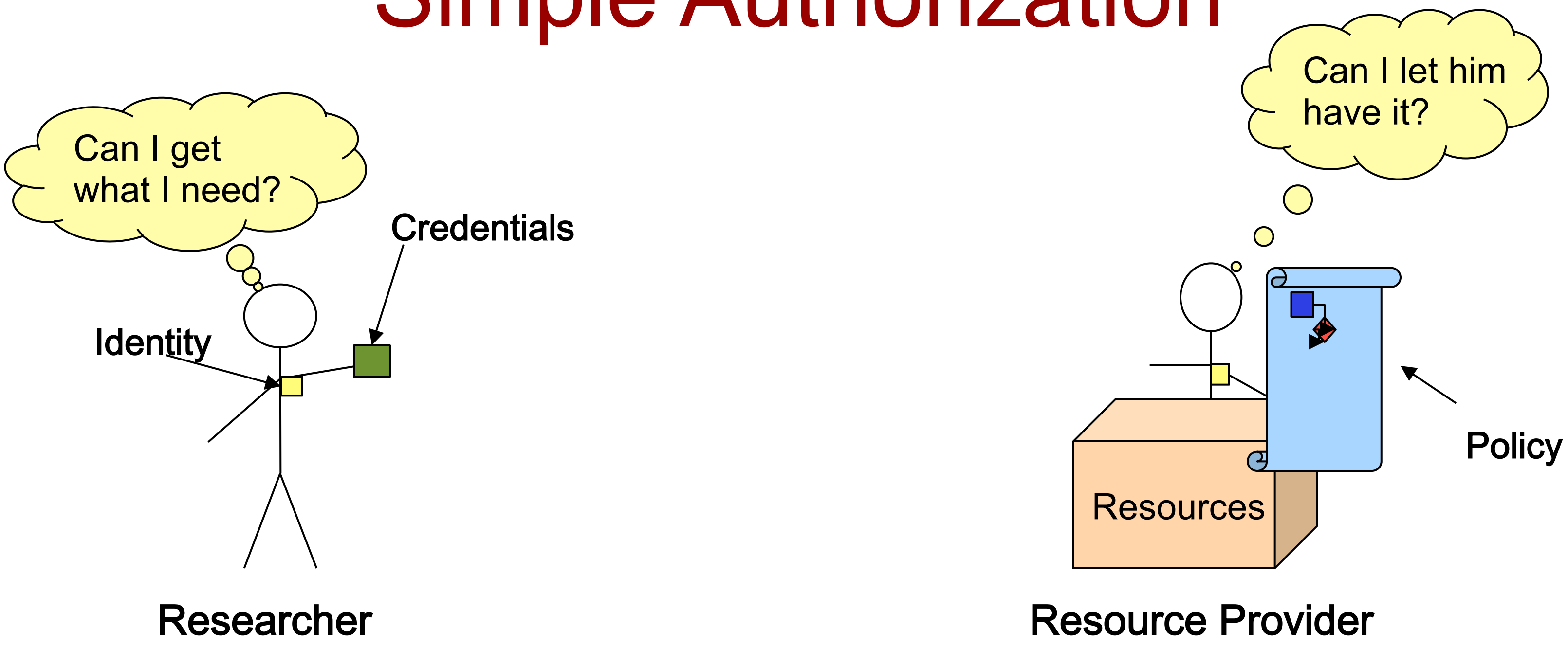
- Every decision should be accountable, leaving a record that is:
  - Transparent: Access is Granted or Denied based upon a definitive set of policy assertions and trusted facts.
  - Auditable: Operators, Policy Makers, Security Authorities, and 3rd Parties may examine logs to determine why a specific decision (access granted or denied) was made.
  - Changes to policy may be reviewed (formally, in advance) to ensure compliance with organizational objectives or external commitments.

What security problems are we solving?

4. Selective Exposure of Policy

- Security Attributes and Policies may reveal sensitive information about individuals or organizations
  - Limiting sharing of attributes and policy rules through selective revelation enables disclosure only when appropriate
  - Policies govern exposure: when, with whom, and under what circumstances attributes and policy relevant information may be exchanged

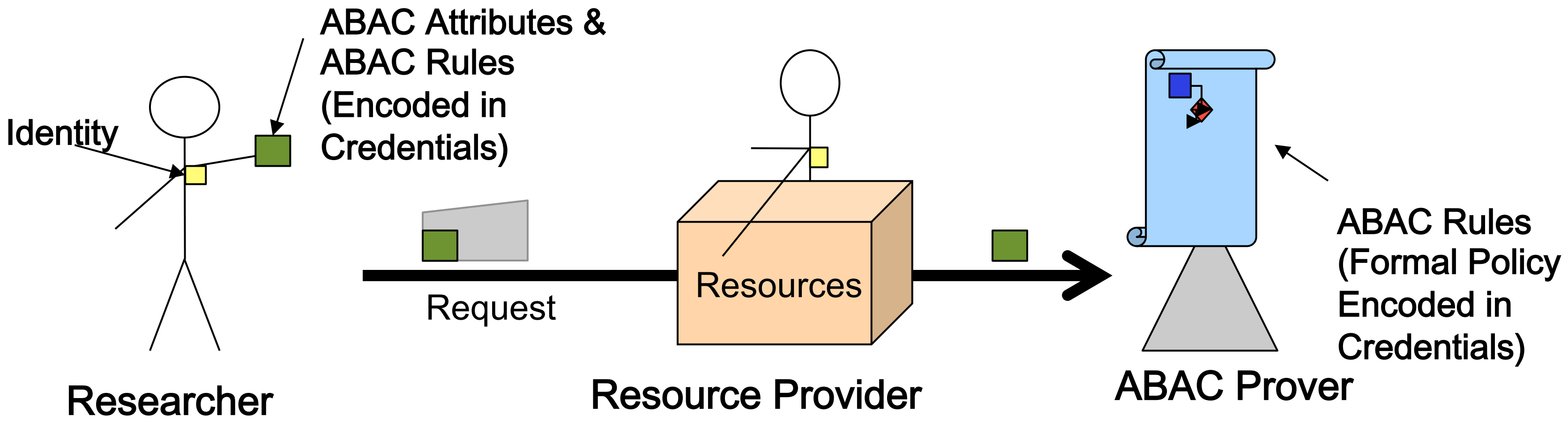
Technology:
Simple Authorization



Applying policy answers these questions. This policy can be simple or ad hoc, but…

- Enforcement mechanisms are tightly integrated
- Policy checks depend on implicit state

Technology:
Attribute Based Access Control


Identity
ABAC Attributes & ABAC Rules (Encoded in Credentials)
Researcher
Request
Resources
Resource Provider
ABAC Rules (Formal Policy Encoded in Credentials)
ABAC Prover

ABAC cleanly separates and defines policy and enforcement

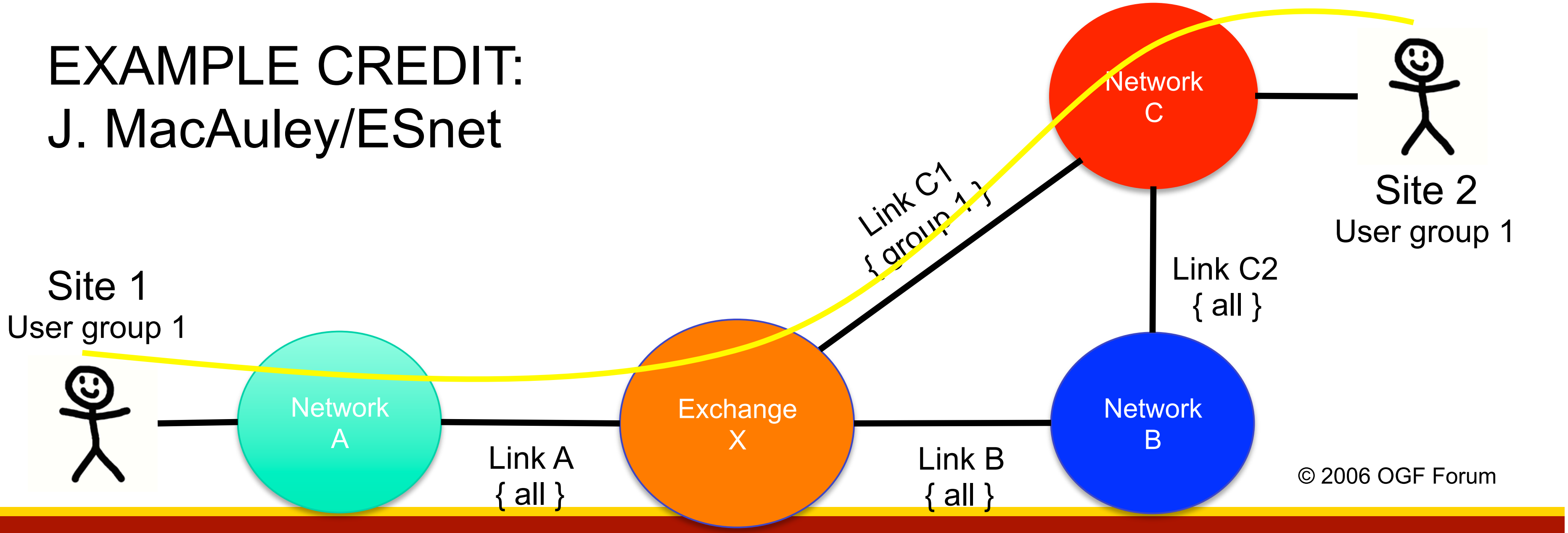
- Attributes and Inference Rules: signed, stored, forwarded
- Enforcement Checks make Explicit Use of information

Resource allocation policies

Restrictions on the path a reservation may take through the network based on the segmentation of allocated resources within the network to specific groups of users.

In the example below, Link C1 is tagged for use by user group 1 only, while all other links are tagged for cooperative sharing. Only users that are members of group 1 may use link C1 in reservation requests.

EXAMPLE CREDIT:
J. MacAuley/ESnet



© 2006 OGF Forum

ABAC Policy Sketch:
User Group1 may use Link C1

X.group1 ← X.admin.group1
C.group1 ← C.admin.group1
(X and C believe admins are those authorized by sites 1 and 2 in ABAC rules. Admins authorize membership in group1.)

X.link(C1).establish(source_network, dest_network, user, [bw], [...])
    ← X.user.group1
C.link(C1).establish(source_network, dest_network, user, [bw], [...])
    ← C.user.group1
(Additional ABAC rules for transitive next hop policy checks, etc.)

What is ABAC?

- An effort to realize attribute based authorization for trust management in a packaged deployable system
- Theoretical roots in trust logic and formal semantics
  - Attribute-Based Access Control investigated under a string of collaborative research projects (DARPA, NSF) with academic and industry collaborators
  - Li, Mitchell, Winsborough. “Design of a Role-Based Trust Management System”, IEEE S&P 2002.
- Refinement and subsequent research culminating in current practical and portable implementation
  - NSF GENI and DHS DETER sponsorship
  - *Libabac-0.1.8* software distribution (2015-03-12)

ABAC Capabilities

- Current capabilities in the latest release
  - Formal Expressive Attribute Logic
  - Expresses authorization policy
  - Used to make authorization decisions
    - Local authorities (``relying parties'') use a combination of *their own* assertions (policy) and *received* assertions (policy and trusted facts) to grant or deny a request
  - Records reasoning of decisions
    - Success: auditable record of decision process
    - Failure: tells why not, suggests path to success
  - Command line and common language bindings
  - X.509 and XML credential formats
- Source, binaries, documentation: http://abac.deterlab.net

Experience

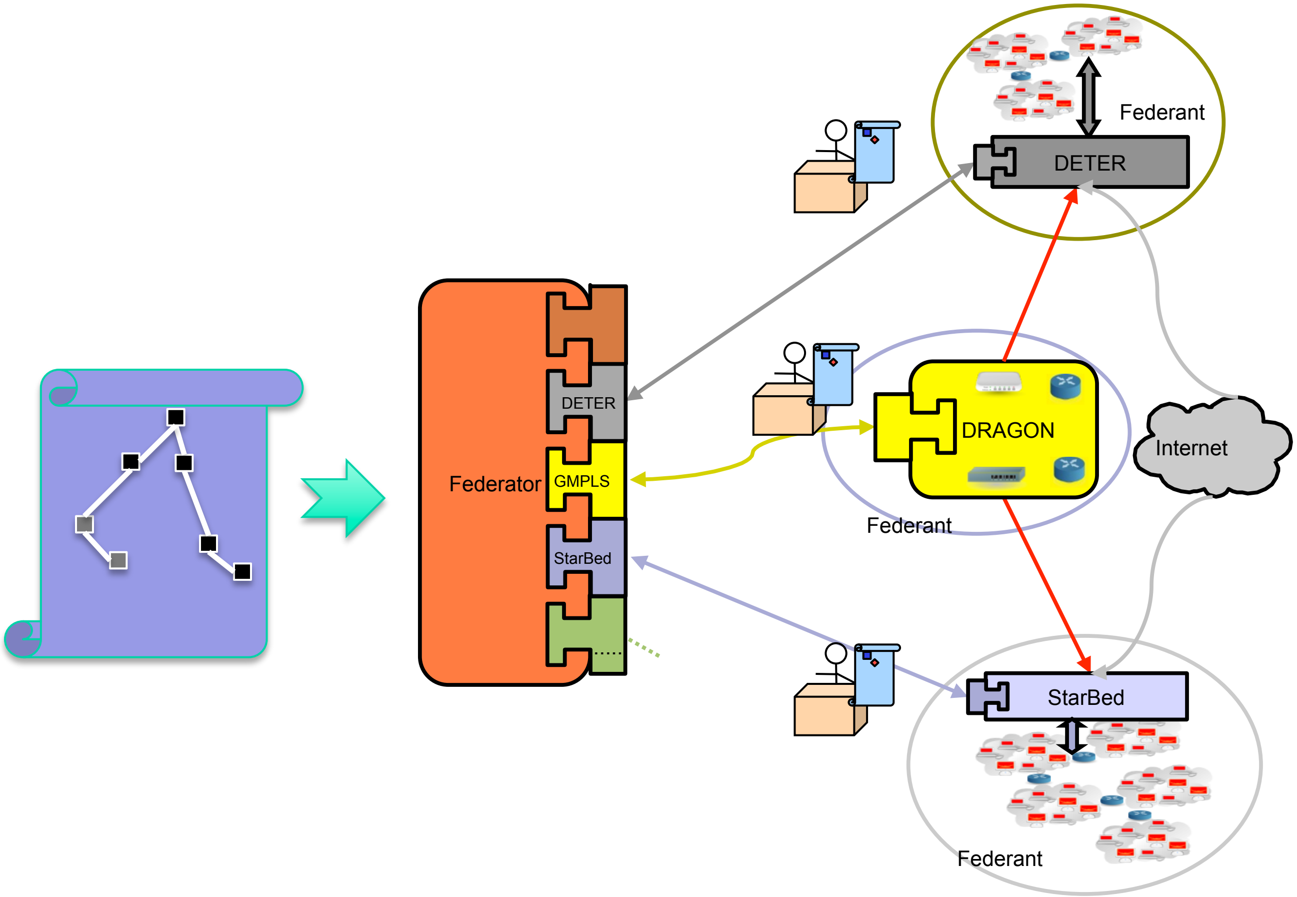
DETER

- Federation Daemon
- Examples: ProtoGENI, Starbed (Japan), Oscars (I2 Provisioning), Desktop Federation Gateway (Any Researcher)

GENI

- Security Policy for Distributed (Federated) Collection of Resources
- Approach used in selected policy enforcement points in Speaks-For scenarios (CloudLab, GENI Desktop) and GENI Clearinghouse

DETER Federation Use Case



GENI Use Case

Delegation and the ``SpeaksFor’’ credential

GENI Authorization must reflect the emerging needs of the research community

Key point: Simple authorization schemes became unwieldy because these approaches do NOT reflect the pattern of use crucial to the GENI project

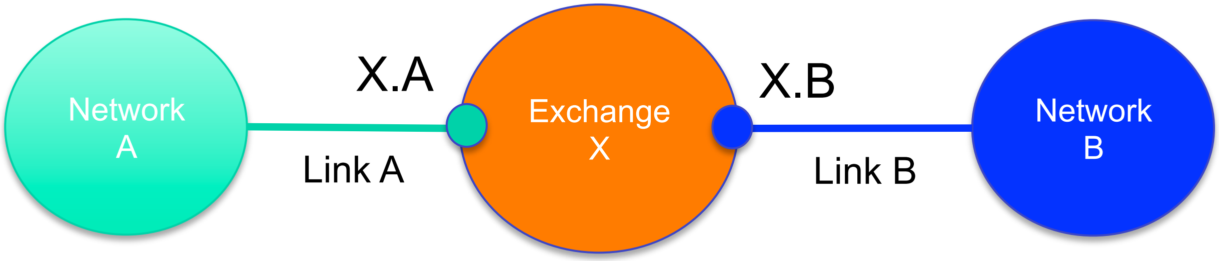
Lessons Learned

- Based on DETER and GENI experience
- Importance of
  - Software fitting into eco-system (build process, library dependencies, range of programming language bindings)
  - Recognizing requirements and serving the needs of the stakeholders

Policy Use Case: Link (Port) Ownership

```
X.establish(A, X, user(U), [bw], […]) ← X.peer.establish(…)
    X.peer ← A.port(LinkA)
    X.peer ← B.port(LinkB)
A.establish( … ) ← "A's policy for use of LinkA"
B.establish( … ) ← "B's policy for use of LinkB"
[One or several ABAC statements, encoded as credentials]
```

EXAMPLE CREDIT:
J. MacAuley/ESnet



Current Focus

Fundamental Software Performing as Discussed

Current Task: Accessibility for Non-Security Experts

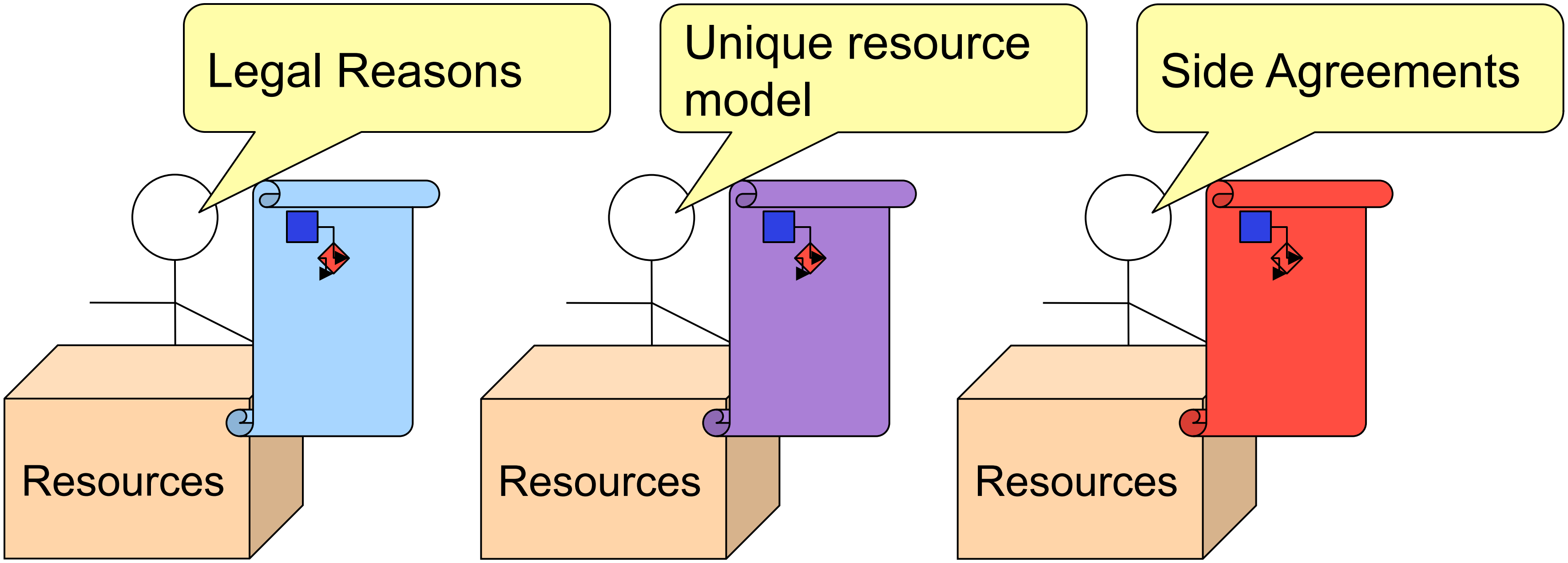
- User Interface Tools and Human Factors
  - Reflect to Community of Users
  - Community-centric Language and Policy Metaphors
  - Adapt the Tools to the Humans
- Vocabularies
  - Policy Concepts and Tools for Tailored Vocabularies
  - Extensible and serving a specific domain or community

Questions

?

Backup

Why Different Policies?



Legal Reasons

Unique resource model

Side Agreements

Resources

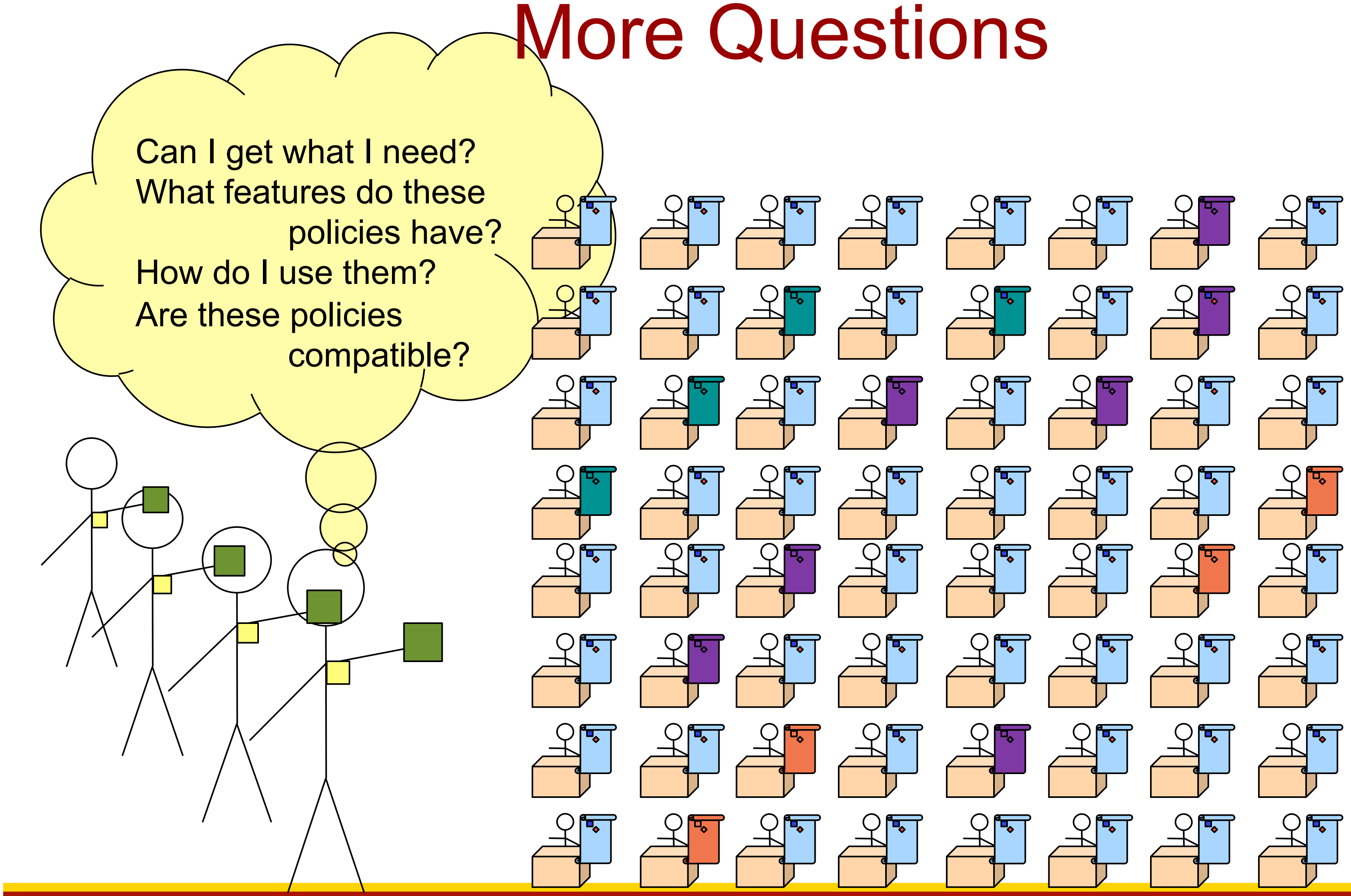
Resources

Resources

Resource Owners and Operators want Researchers to use their Facilities

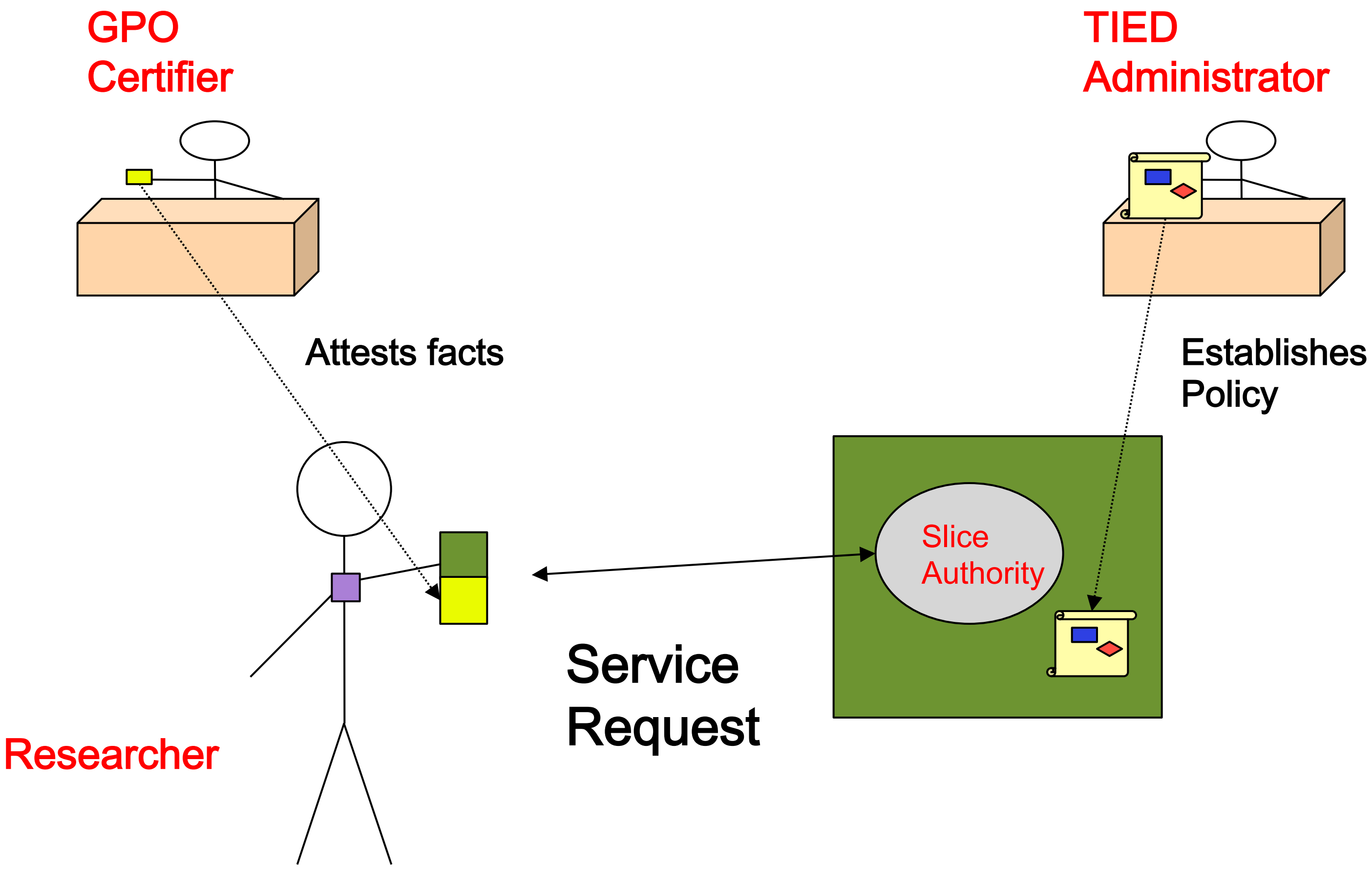
Need a Basis for Analyzing and Creating Many Policies

More Users and More Servers, More Questions



Can I get what I need?
What features do these policies have?
How do I use them?
Are these policies compatible?

ABAC Principals



Attested Attributes

Attribute name: Principal.Role

- Principals attest attributes about principals
  - Principal has *attribute* ↔ Principal in *set*
  - ABAC syntax: Q.admin ← P
- Each Principal Defines An Attribute Space
  - P.admin differs from Q.admin
  - Each Principal Controls Its Attribute Space
- Attributes can have parameters
  - Q.owner(chevy)

Rules to Derive Attributes

Direct connection

- Q says "P assigns Q.friend by assigning P.friend"
  - "P's friends are Q's friends"
  - Controlling Principal (Q) Delegates to a Principal
- ABAC syntax: Q.friend ← P.friend

Indirect connection

- Q says "anyone with P.friend can assign Q.friend by assigning friend in their namespace"
  - "Friends of P's friends are Q's friends"
  - Controlling Principal (Q) Delegates to a set of principals
- ABAC syntax: Q.friend ← (P.friend).friend