Federation in GENI

Draft proposal – Comments invited

GEC11 – Denver, Colorado

Aaron Falk

26 July 2011

Sponsored by the National Science Foundation

Outline

- What is the GENI Federation?
- Federation Member Responsibilities
  - GENI Clearinghouse
  - GENI Meta-Operations
  - Aggregates
  - Project Leaders & Experimenters
  - Identity Portals
  - Opt-In Users (fuzzy)
- Examples

Federation in GENI

- **Federation:** An organization or group within which smaller divisions have some degree of internal autonomy

- The GENI federation is an NxM partnership of experimenters and aggregates that exists to make it easier for all to do research than would otherwise be possible.
  - Members only give away the local autonomy essential to making the federation work
  - Aggregates benefit from identity vetting, operational support, assistance with forensics
  - Experimenters benefit from access to new kinds of resources, unified authentication/authorization, resource discovery, help desk, stitching, measurement infrastructure

- The federation works if all of its members benefit. To achieve this imposes requirements on federation members. This presentation is about those requirements.

Design Principles for Federation

- **GENI should be attractive to experimenters**
  - Experimenters should gain access to resources that would otherwise be difficult to acquire
  - It should be easy for experimenters to use GENI
  - The GENI Federation should be able negotiate with other federations as a body, e.g., to exchange access to resources
- **GENI should be attractive to aggregates**
  - It should be easy for aggregates to join & participate
  - Aggregates should retain autonomy
  - Federation should not be exclusive
- **Funding agencies (e.g., NSF) should perceive the benefits outweigh the risks**
  - Accountability of actions is important; For example, allocated resources should be associated with a responsible individual
  - Give special attention to security for resource allocation & accountability trail (i.e., consider the risk of entity subversion)

Some New Terms

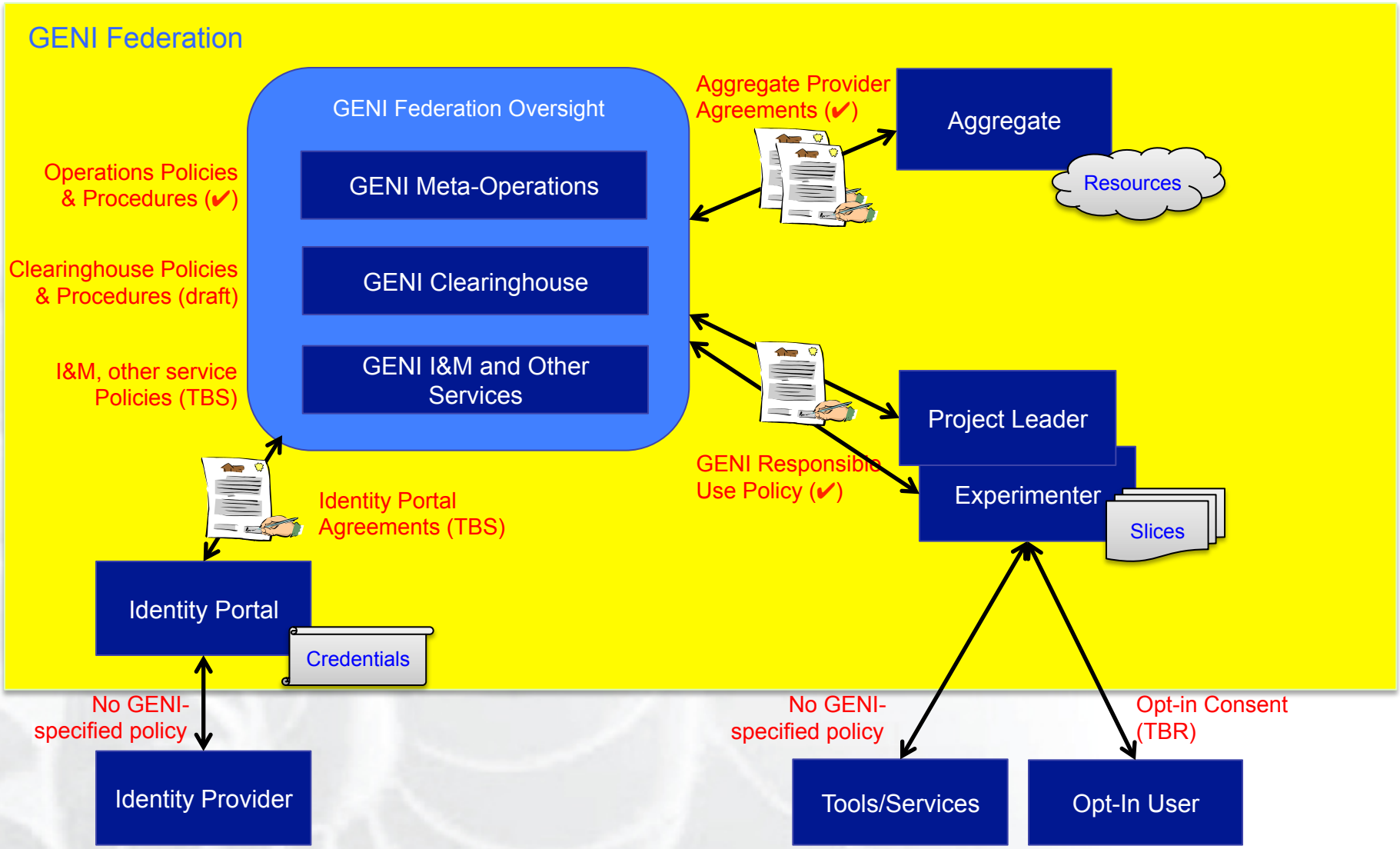
- **Identity Provider:** an entity who can assert identity attributes without further proof
- **Identity Portal:** a system that issues identity credentials; may rely on external identity providers
- **GENI Project:** a grouping of experimenters and slices working on a common effort (think 'experiment'). May have multiple slices concurrently and over time.
- **Project Leader:** The actor who is ultimately responsible for the behavior of a GENI project

NB. 'Project' is used to name GPO subcontracts but use of this term is expected to diminish over time.

Federation Governance

- The GENI federation consists of several entities all joined by a set of mutually beneficial agreements
- Policies & agreements are established by a *GENI Oversight Group*
  - –This group represents the interests of the members (& funders)
- Oversight is currently provided by the GENI Project Office
  - –GPO oversight is a temporary arrangement while the federation comes into being
  - –Later oversight will be performed by a governing council
- The GENI Clearinghouse, Meta-Operations Center, and other federation-sponsored functions operate under policies set by the GENI Oversight Group

Agreements in & around the GENI federation

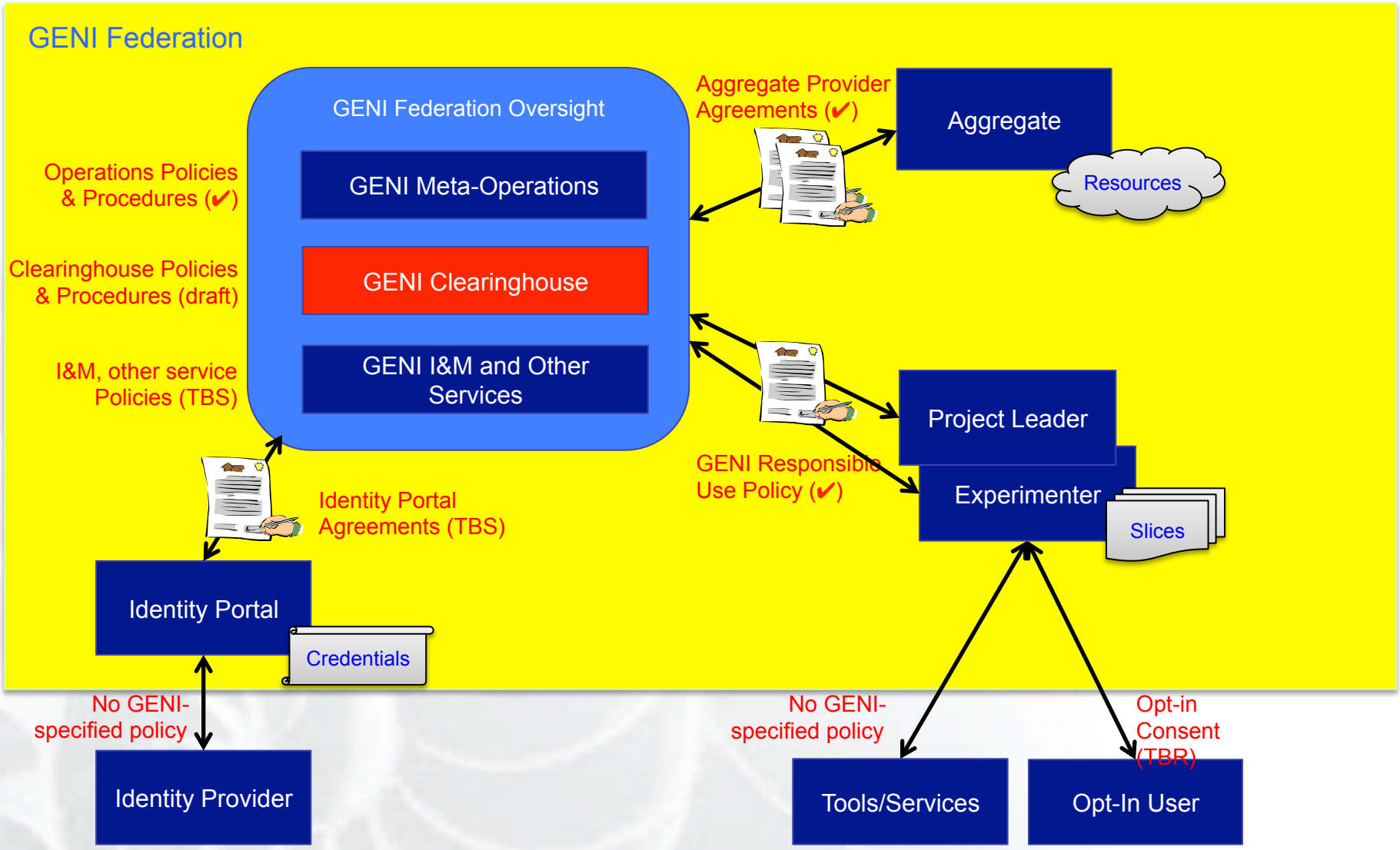


(✔) = early policy/agreement is in place today

Outline

- What is the GENI Federation?
- Federation Member Responsibilities
  - GENI Clearinghouse
  - GENI Meta-Operations
  - Aggregates
  - Project Leaders & Experimenters
  - Identity Portals
  - Opt-In Users (fuzzy)
- Examples

GENI Entity: Clearinghouse



(✔) = early policy/agreement is in place today

GENI Entity: Clearinghouse

- The GENI Clearinghouse provides a trust anchor (e.g., CA) and supporting services enabling federation-wide policies and mechanisms to function.
  - The Clearinghouse (solely) creates projects, issues project leader credentials, and provides GENI endorsement to registered slices
  - The Clearinghouse provides trustworthy services permitting aggregates to outsource some functions if they choose (e.g., transaction logging)
  - The Clearinghouse provides some other non-exclusive services which will help GENI function (e.g., stitching, discovery)

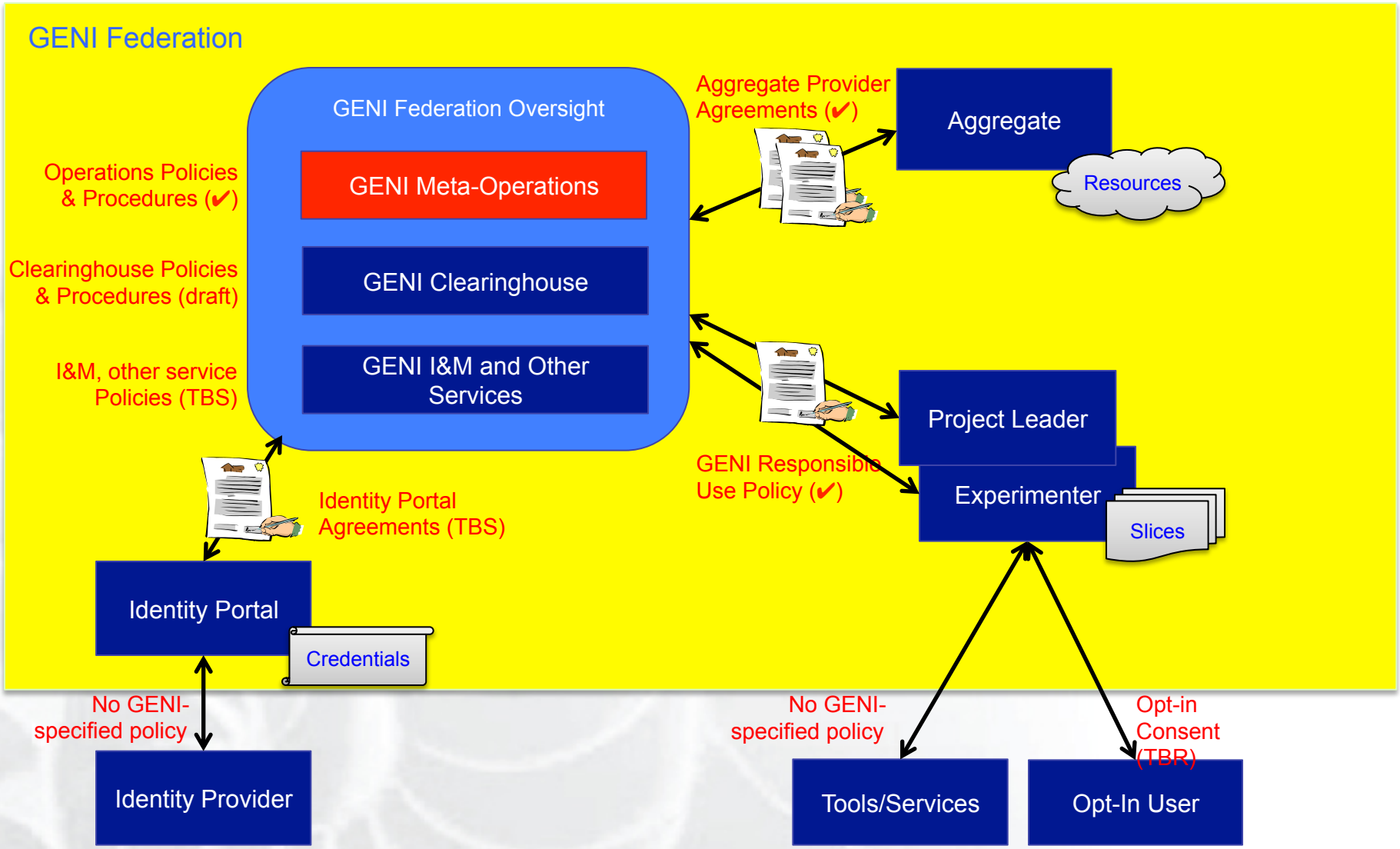
- The Clearinghouse operates according to policies and procedures approved by the GENI Oversight Group.

Clearinghouse Responsibilities

- **GENI Clearinghouse responsibilities** that flow from making the Federation attractive (e.g., safe and accountable) to experimenters, resource providers and funders
  - Authorize & register projects, issue project leader credentials
  - Operate a slice authority: endorse & register GENI slice credentials
  - Authorize & register aggregates, issue aggregate credentials
  - Operate services supporting
    - federation-wide resource allocation limits (e.g., proxying aggregates & issuing RSpec endorsements)
    - record-keeping (e.g., robust transaction logs & parsing)
  - Provide an authoritative accountability trail of resource allocation
  - Keep up-to-date records for identities, projects, slices

- **The GENI Clearinghouse may also**
  - Operate an identity portal that can issue & manage GENI identity credentials
  - Operate non-exclusive services enabling discovery & stitching
  - Create slice credentials

GENI Entity: Meta-Operations



(✔) = early policy/agreement is in place today

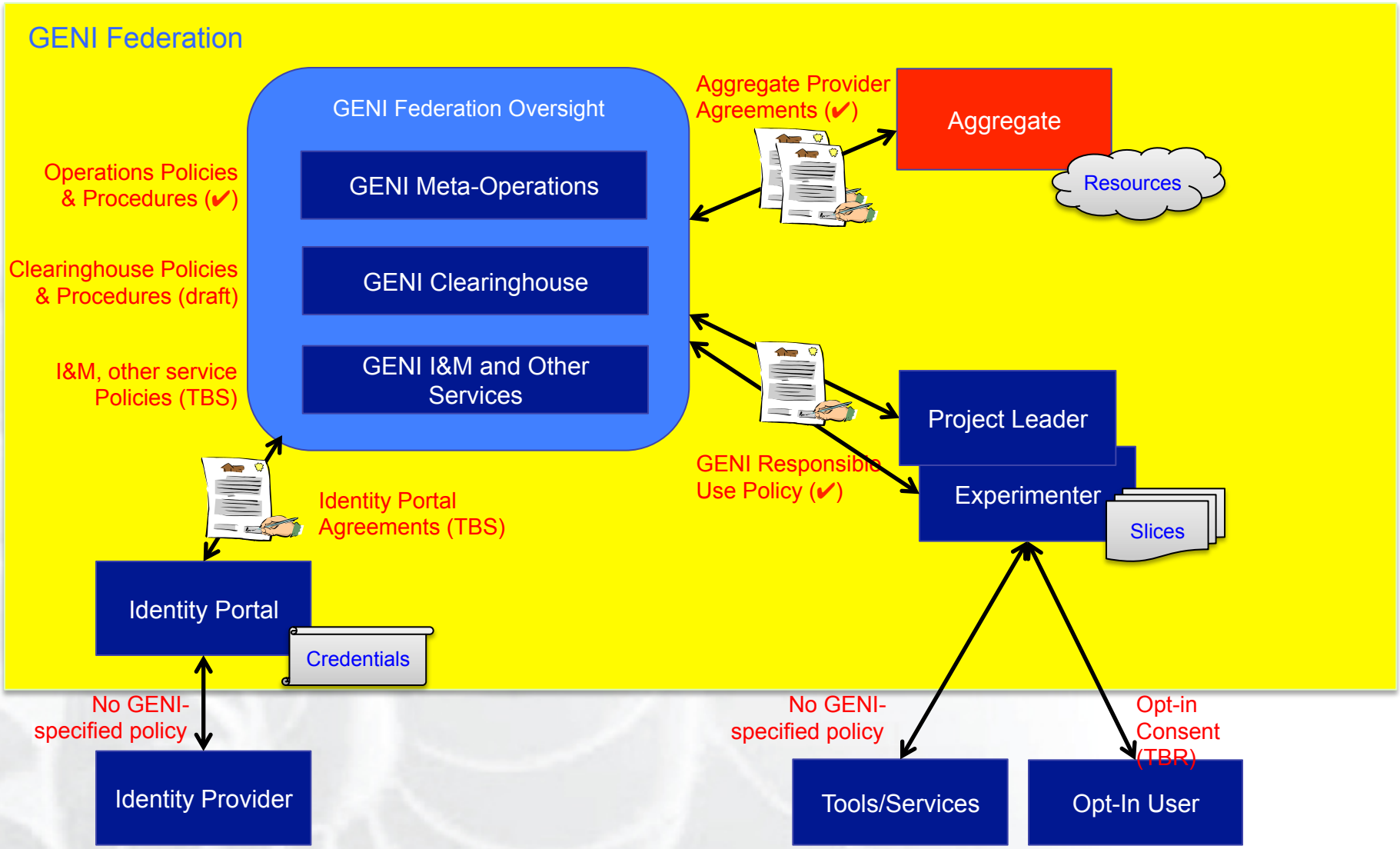
GENI Entity: Meta-Operations

- GENI Meta-Operations
  - **provides operational support** to aggregate operators and experimenters for issues broader than any single entity.
  - **presents a public interface** for operations-related communications.

- Responsibilities
  - Collect & report operational statistics
  - Facilitate trouble resolution between federation members, experimenters; including emergency stop, incident response, and legal & law enforcement requests (LLR)
  - Notify affected members of outage events
  - Operate an experimenter help desk

- The GENI Oversight Group is responsible for Meta-operations fulfilling its responsibilities.

GENI Entity: Aggregate



(✔) = early policy/agreement is in place today

GENI Entity: Aggregate

- An **aggregate** is a system containing a collection of resources under common administration running an aggregate manager

- An aggregate may
  - Be a single computer, testbed, or a complex multi-institution system.
  - Be unattended or have 24x7 operations staff
  - Dedicate some resources for non-GENI use

- Aggregates will include actors who can make agreements with the federation, implement policies, and provide operational support

Aggregate Responsibilities (1)

These responsibilities are geared toward making the federation more attractive to users (by making allocation fairer and cross-aggregate capabilities available) and more attractive to resource providers (by making it safer to share resources).

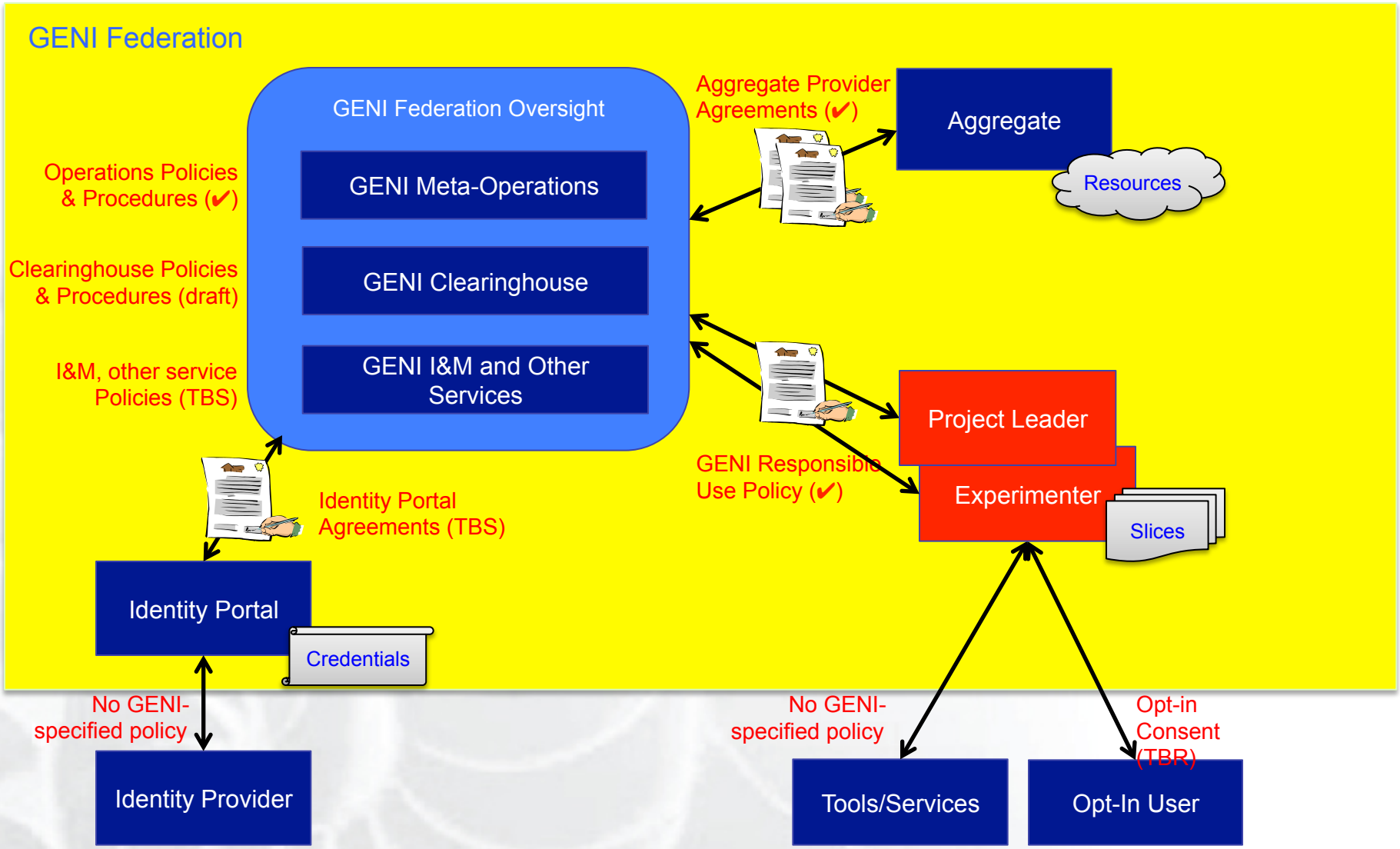
- **Make federation more attractive to experimenters**
  - Make a best effort to describe & provide available resources
  - Recognize experimenters with GENI credentials
  - Discover and apply federation-wide resource allocation policy
  - Operate instrumentation & measurement functions (if possible)
  - Operate network stitching functions (as appropriate)
    - Preferably connect at layer 2

NB. A draft Aggregate Provider agreement exists today. Some of these responsibilities are new, i.e., not in the current agreement.

Aggregate Responsibilities (2)

- **Make the federation attractive to resource providers**
  - Help answer "Who is responsible for activities on this resource?"
    - Minimally, accept only transactions that have been proxied through the GENI Clearinghouse, which will maintain logs.
    - Alternatively, maintain local resource allocation transaction logs (meeting federation requirements for reliability, retention, and sharing)
  - Help answer "Who is (probably) responsible for this traffic?"
    - Minimally, be able to trace Internet-bound traffic to a GENI slice; i.e., "What slice is attacking chase.com?"
    - If feasible, be able to map other kinds of traffic (e.g., VLAN) to a GENI slice; i.e., "What slice is melting this switch port?"
  - Follow security best practices, e.g., actively monitor & secure site
  - Cooperate with GENI Meta-Operations on trouble resolution
    - Share some monitoring data with GENI Meta-Operations
    - Provide contact information to GENI Meta-operations
    - Implement GENI emergency stop procedures

GENI Entities: Experimenter, Slice, Project, Project Leader



(✔) = early policy/agreement is in place today

GENI Entities: Experimenter, Slice, Project, Project Leader

- A **slice** is the binding of resources to experimenters.
- A **project** is an abstraction providing a single point of accountability for groups of experimenters and slices.
  - Every GENI slice is associated with one project
  - Projects may include multiple slices (concurrently or over time).
- A **project leader** is an actor responsible for a project and the activities in any associated slices.
  - Project Leader can delegate the ability to create and act on slices.
- An **experimenter** is an actor to whom the Project Leader has delegated privileges to act on a slice

- Controls are placed on Projects to help the Federation provide 'safety' benefits to resource providers (& funders)
  - GENI may establish federation-wide policies that govern what a slice or project may do.
  - Only one project leader per project
  - The PL role can change over time but is not delegatable

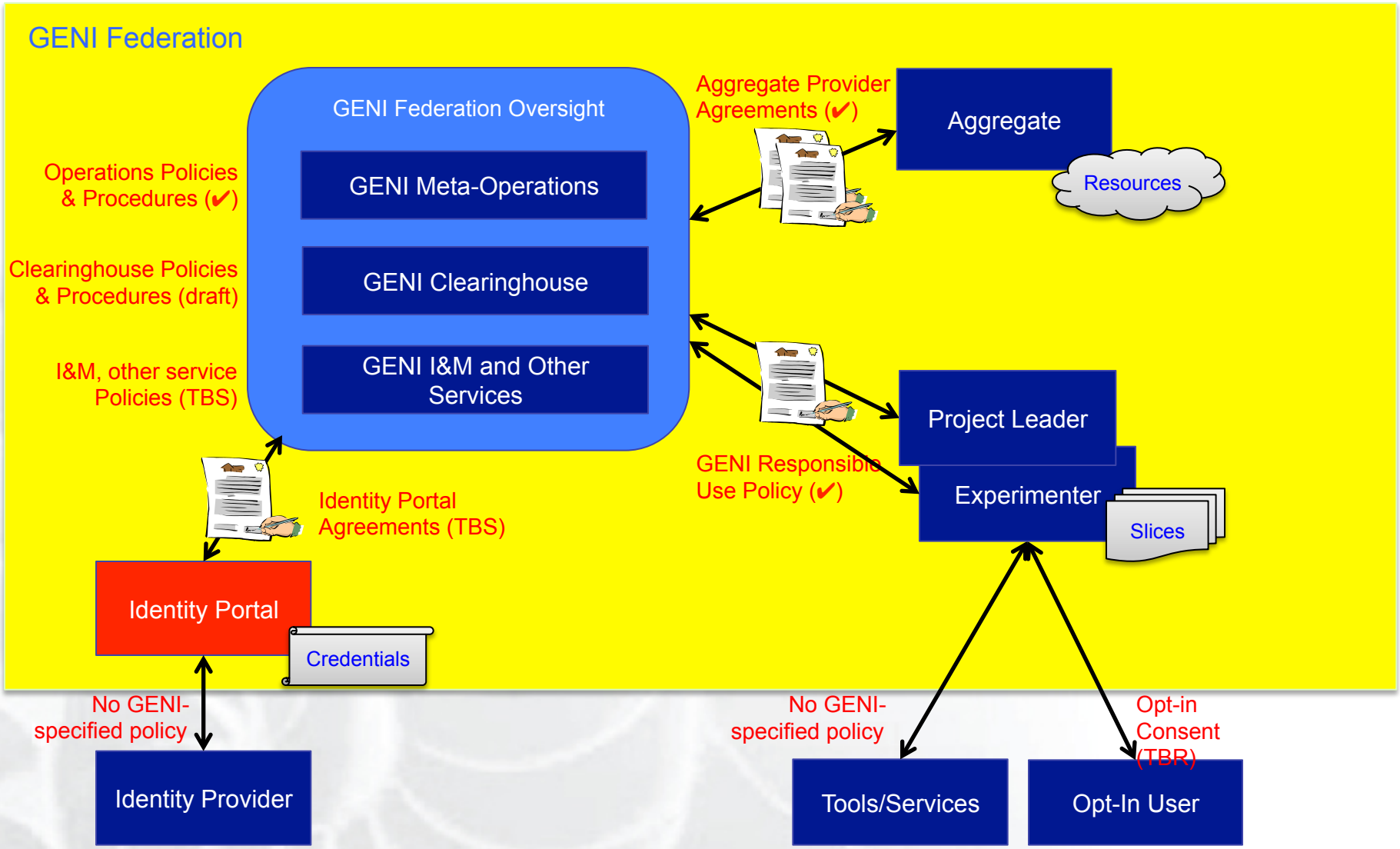
NB. 1. The policy for who can be a Project Leader is out of scope for this talk. 2. May want to add 'experimenter groups' within a project to help manage privileges. Doesn't change the concepts above.

Experimenter Responsibilities

- Obtain valid credentials
  - Keep contact information (e.g., email address) up to date
- Behave responsibly
  - Be responsible for software running in their slice
  - Secure software and systems under their control
  - Adhere to common network etiquette
  - Avoid disruption of shared infrastructure
  - Debug experiments before deploying in GENI
  - Cooperate in resolving disruptions or bad behavior
- Cite GENI in publications.
- Support opt-in policies (TBS)

NB. A draft Experimenter Recommended Use Policy exists today. Some of these responsibilities are new, i.e., not in the current agreement.

GENI Entity: Identity Portal



(✔) = early policy/agreement is in place today

GENI Entity: Identity Portal

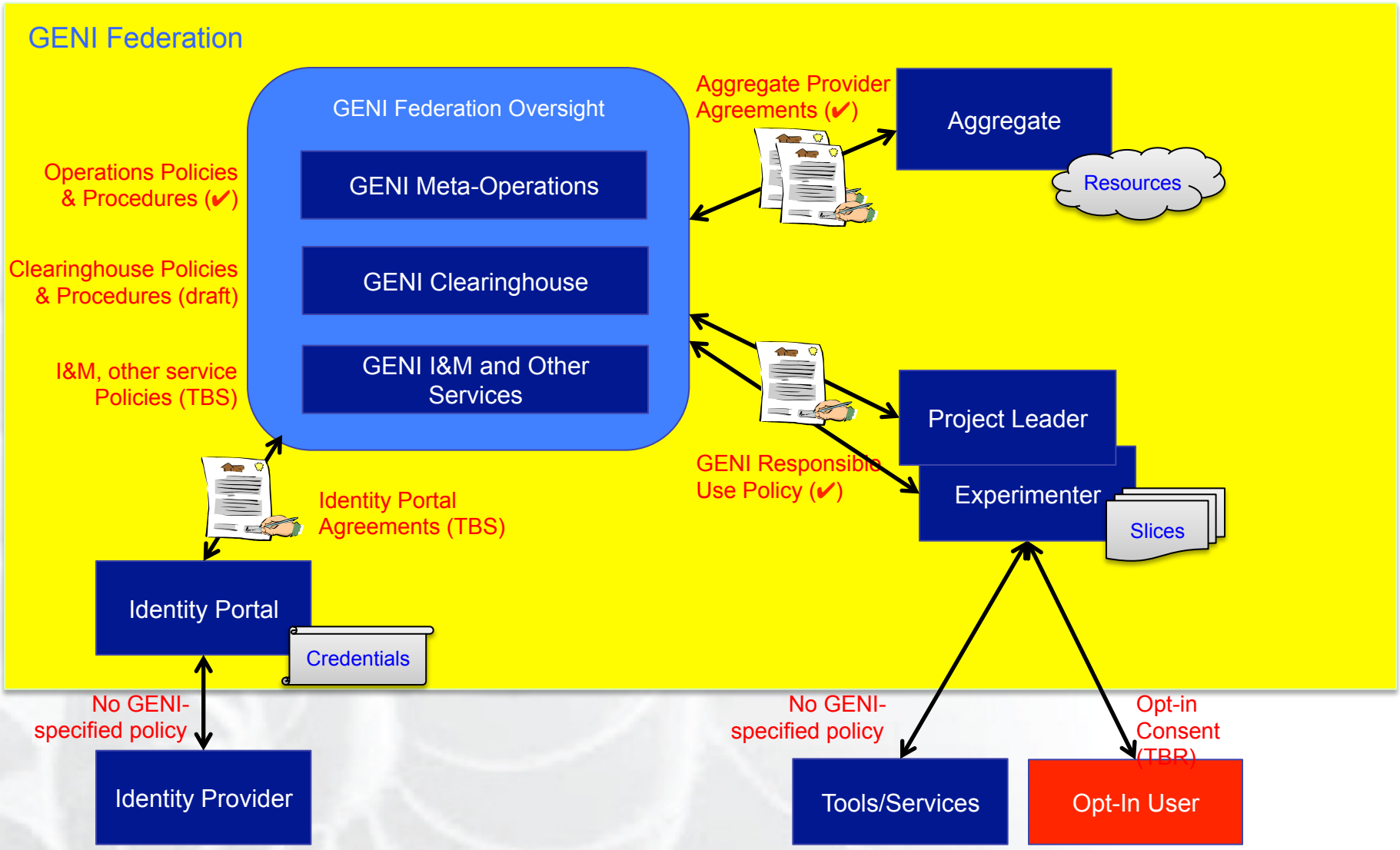
- Identity portals issue credentials in a common format that identify individuals.
  - Common credentials benefit experimenters by providing a single token recognized throughout the Federation (& possibly elsewhere), while providing some privacy in interactions with resource providers
  - Common credentials benefit resource providers by providing an accountability trail that allows identification of the individuals acting on federated resources
  - Identity Portals maintain registries with identity and contact information
    - Identity Portals are likely to rely on external identity providers
  - The GENI Federation may have multiple Identity Portals operating under policy & procedures established by the GENI Oversight Group

NB. Should consider what happens should an Identity Portal go rogue.

Identity Portal Responsibilities

- Issue credentials
  - Issue a cryptographic object in a standard format containing the credential
  - Obtain consent to comply with relevant policies (e.g., Experimenter RUP)
  - Verify the identity attributes which will be credentialed
  - Void credentials through CRLs, OCSP, expiration dates, or other means, when they are no longer valid
- Keep records up to date
  - Allow experimenters to revise or update information in credentials or used to obtain them
  - Keep authoritative records of who credentials have been issued to and the date of issue

GENI Entity: Opt-In Users



(✔) = early policy/agreement is in place today

GENI Entity: Opt-In Users

KNOWN TO BE FUZZY

- Opt-in users are unlikely to be GENI Federation members
- Experimenters may be responsible for opt-in interactions
- The federation has a stake in opt-in success and growth
- The federation will need to develop supporting tools and opt-in policies with buy-in from campuses and experimenters

- Example experimenter responsibilities regarding opt-in users:
  - Follow published best practices
  - Be responsive to complaints
  - Honor opt-out / blacklisting
  - Keep logs private
  - Be explicit about how data is collected, analyzed, published

Outline

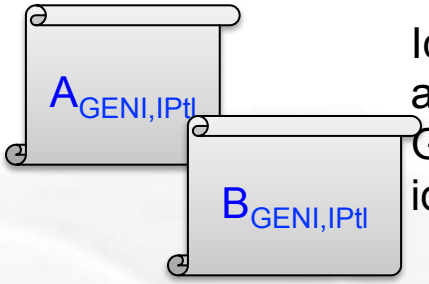
- What is the GENI Federation?
- Federation Member Responsibilities
  - GENI Clearinghouse
  - GENI Meta-Operations
  - Aggregates
  - Project Leaders & Experimenters
  - Identity Portals
  - Opt-In Users (fuzzy)
- Examples

How it works – a simple example

1. Project Leader and Experimenter obtain identity credentials from a trusted identity portal, possibly the GENI Clearinghouse, after consenting to follow the GENI Experimenter RUP.
2. Project Leader creates a project at the Clearinghouse, describes planned use; the Clearinghouse approves the project and issues a GENI Project Leader credential
3. An Experimenter, with Project Leader's delegation, mints a slice possibly using a service at the Clearinghouse
4. The slice is registered at the Clearinghouse w/contact info; the request is verified and the Clearinghouse endorses the slices, creating a GENI slice credential
5. The Experimenter sends a request (w/an RSpec) for resources at a particular aggregate and provides Experimenter and GENI slice credentials
   - Some aggregates will only accept requests via the Clearinghouse, as a matter of policy; the Clearinghouse logs the transaction and verifies the request meets Federation policy
   - Some aggregates will accept requests directly from Experimenters, as a matter of policy; the Experimenter consults the Clearinghouse on whether the request meets Federation policy and is issued an endorsement which can be presented to the aggregate
6. The Experimenter gets a response to the request
7. If the request did not route through the Clearinghouse, the aggregate asynchronously updates the Clearinghouse transaction logs of the allocation

Credentials in GENI

Identity Credentials

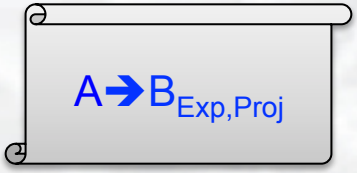


Identifies holders A and B, issued by GENI-authorized identity portal IPtl

Project Leader Credential

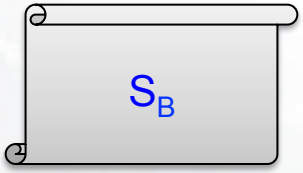
Identifies A as Project Leader of project Proj. By policy, only the GENI Clearinghouse can issue a PrL credential.

Privilege Delegation

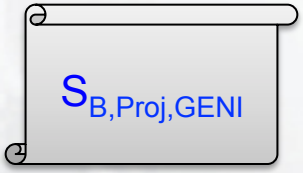


Privilege delegation: A delegates to B the privileges Exp for project Proj

Slice Credentials



Slice: identifies slice S and binds slice to slice creator B



GENI Slice credential: when registered, the GENI Clearinghouse endorses slice S as a GENI slice

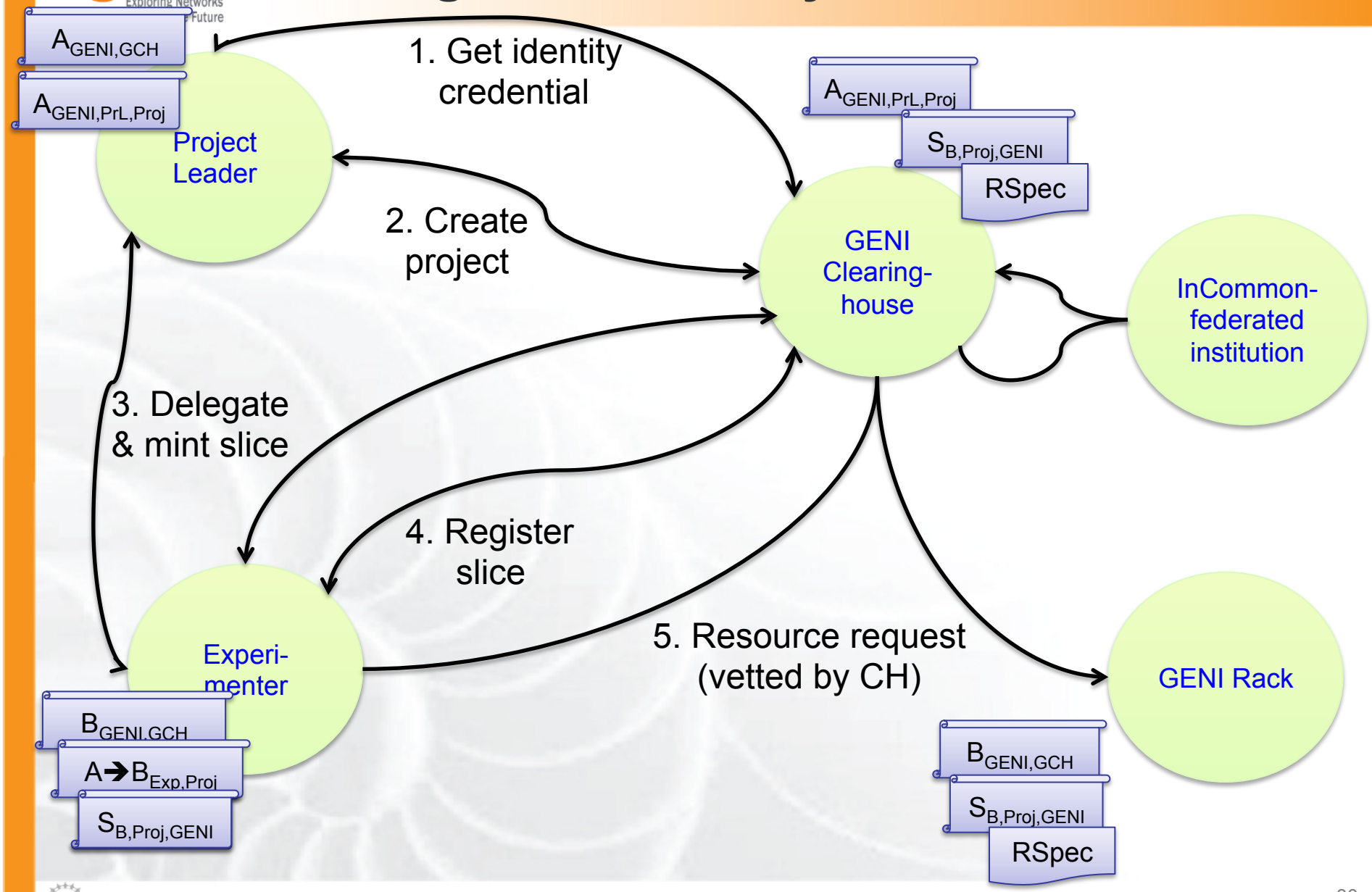
NB. Aggregates & operators will require credentials as well.

Federation Use Case 1: GENI Rack Aggregate

- Scenario: experimenter wishes to use identity credentials from the GENI Clearinghouse identity portal ("GCH" in the diagram) and obtain resources on a GENI Rack
- The Rack only accepts requests from GENI authorized experimenters and only via the Clearinghouse
- The Clearinghouse obtains information from the Experimenter's institution via Shibboleth/InCommon as an input to the credential generation process
- The GENI Clearinghouse gathers some additional information from the Experimenter and validates it before issuing an identity credential
- The GENI Clearinghouse logs transactions & filters requests before forwarding to the aggregate based on federation-wide policy

Best viewed in PPT presentation mode

Clearinghouse Identity Portal & GENI Rack



Federation Use Case 2: Emulab as Aggregate & Identity Portal

- Scenario: experimenter wishes to use Emulab-issued identity credentials to create a GENI slice that includes Emulab and GENI Rack resources

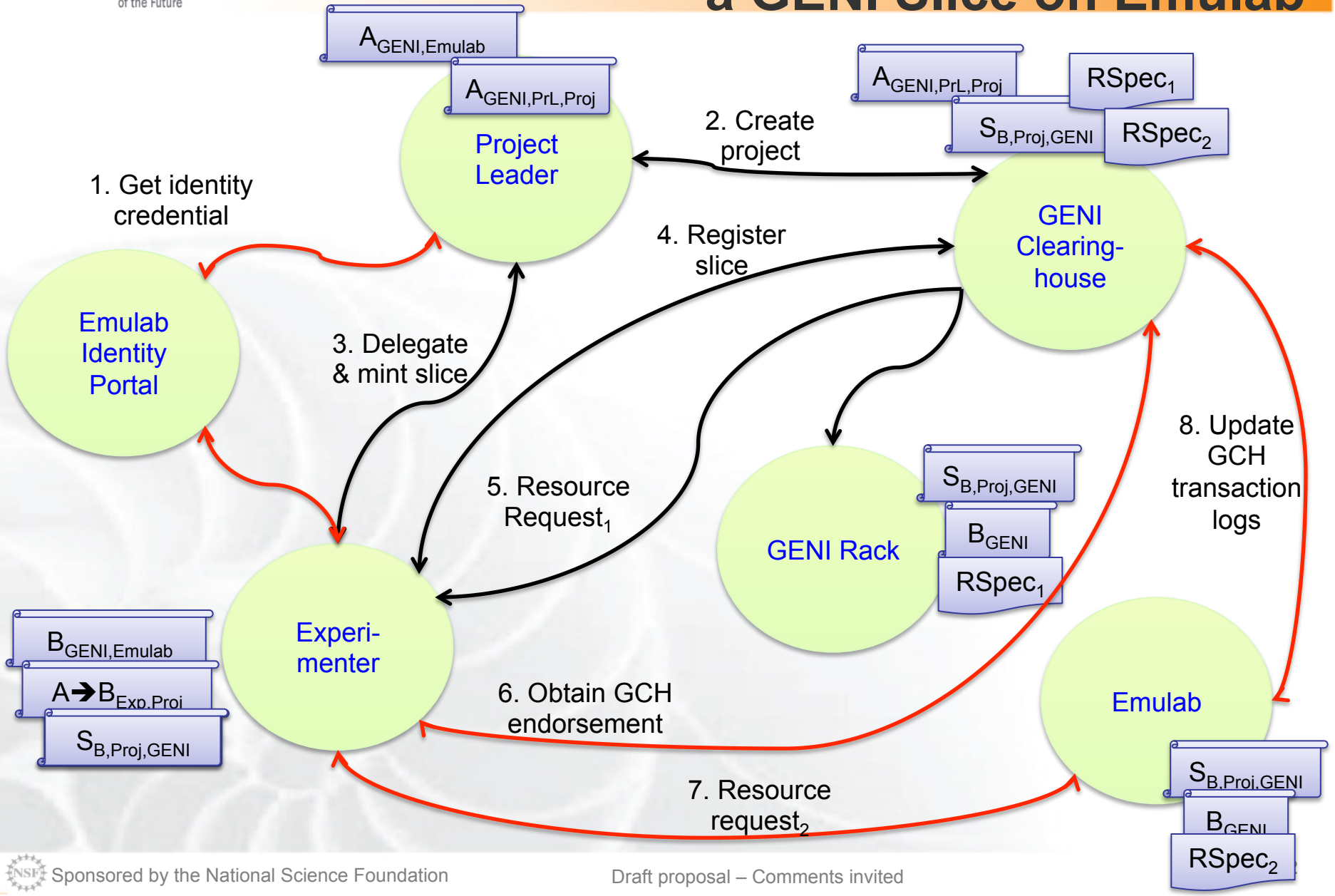
- Emulab creates user accounts for Experimenters and has an identity portal agreement with GENI
  - Agrees to meet GENI identity portal & registry standards
  - Is provided with signatures/software to generate valid GENI identity credentials
  - Obtains Experimenter consent to follow the GENI RUP before issuing credentials

- Emulab prefers to accept requests directly from experimenters
  - Experimenter obtains a endorsement from the Clearinghouse which indicates a request meets federation resource allocation policy
  - Emulab updates the GENI Clearinghouse transaction log asychronously with resource allocations

- Emulab also permits users without GENI credentials to obtain its own resources

Best viewed in PPT presentation mode

Emulab Experimenter creating a GENI Slice on Emulab



Federation Use Case 3: Federation-wide Sharing Agreement with a Non-GENI Federation

- Scenario: An agreement is established between the GENI Oversight Group and a non-GENI Federation (NGF)
  - allows a limited number of experimenters with GENI credentials to obtain NGF accounts and access a limited amount of NGF resources
  - allows a limited number of experimenters with NGF credentials to obtain GENI projects and access a limited amount of GENI resources
- Notes:
  - NGF is both an aggregate (or aggregate of aggregates, most likely) and an identity portal. Assume it uses a non-interoperable control plane.
  - NGF aggregates have their own operations.
  - GENI Meta-operations assists/coordinates in response to incidents and LLR issues
  - GENI Clearinghouse issues a limited credentials which will work on NGF to GENI experimenters, limits NGF usage of GENI, and collects operational statistics on cross-federation usage.
  - NGF has the option of operating a GENI identity portal or providing NGF credentials to its experimenters that they can use when requesting GENI credentials from the Clearinghouse

NB. This is just a thought exercise to illustrate only a single type of federation is needed.

geni
Exploring Networks of the Future

Questions?

Open Issues

- Need agreement on endorsement formats and mechanisms to be used for federation-wide policy checking
- End-user Opt-in:
  - Who is responsible for the relationship with opt-in users? (experimenters?) Who wants to be party to any consent agreements? What is the involvement of campus IT? What records need to be kept? By whom? And where?
- Need to security review, e.g., consider if Identity Portal is subverted
- Need to define operator & aggregate credentials

Other Notes

- Clearinghouse might also host a slice ‘mail aliasing’ service