

Introduction to GENI Architecture: Federated Trust Perspective

Aaron Helsing for Marshall Brinn,
GPO

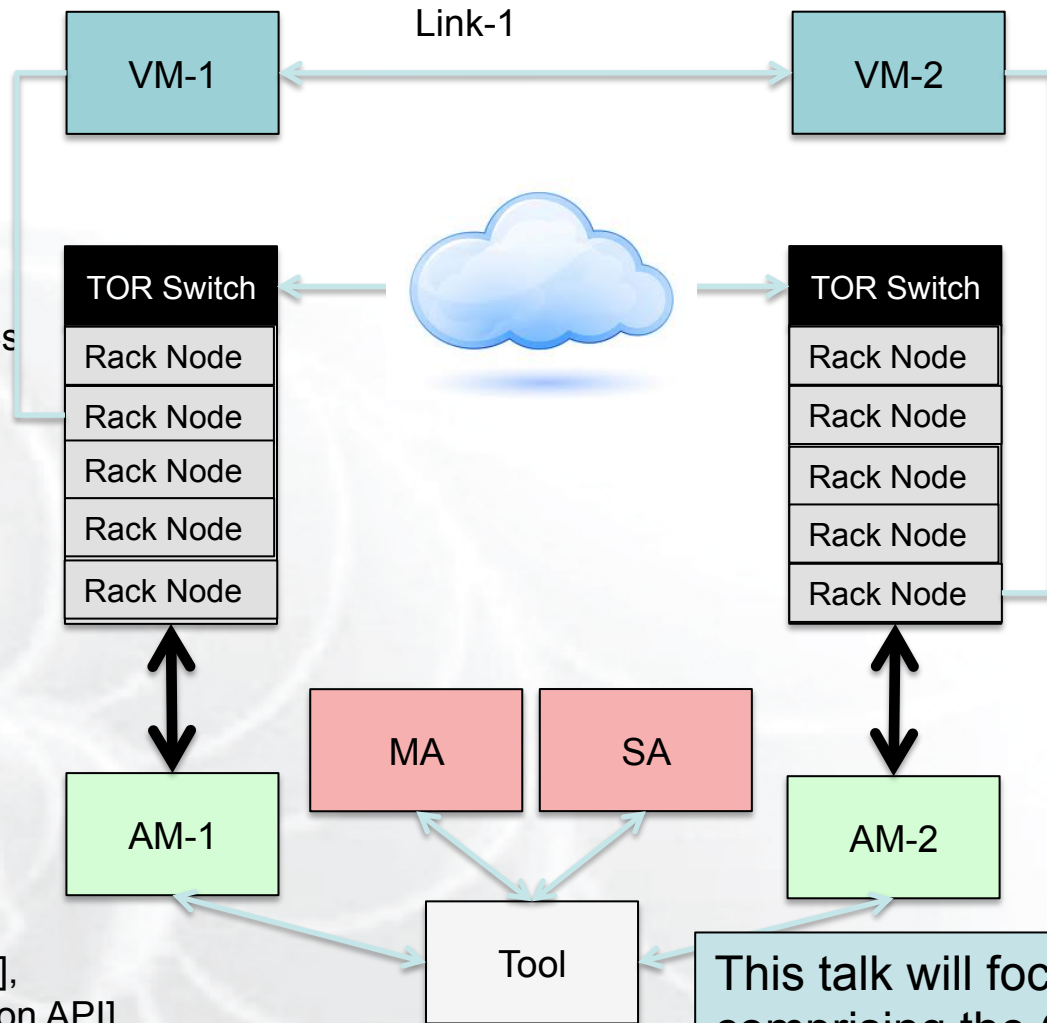
GEC23: June 16, 2015

Viewing GENI at Different Planes

Topology Plane:
Nodes, links

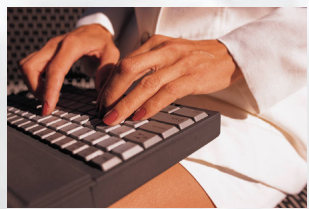
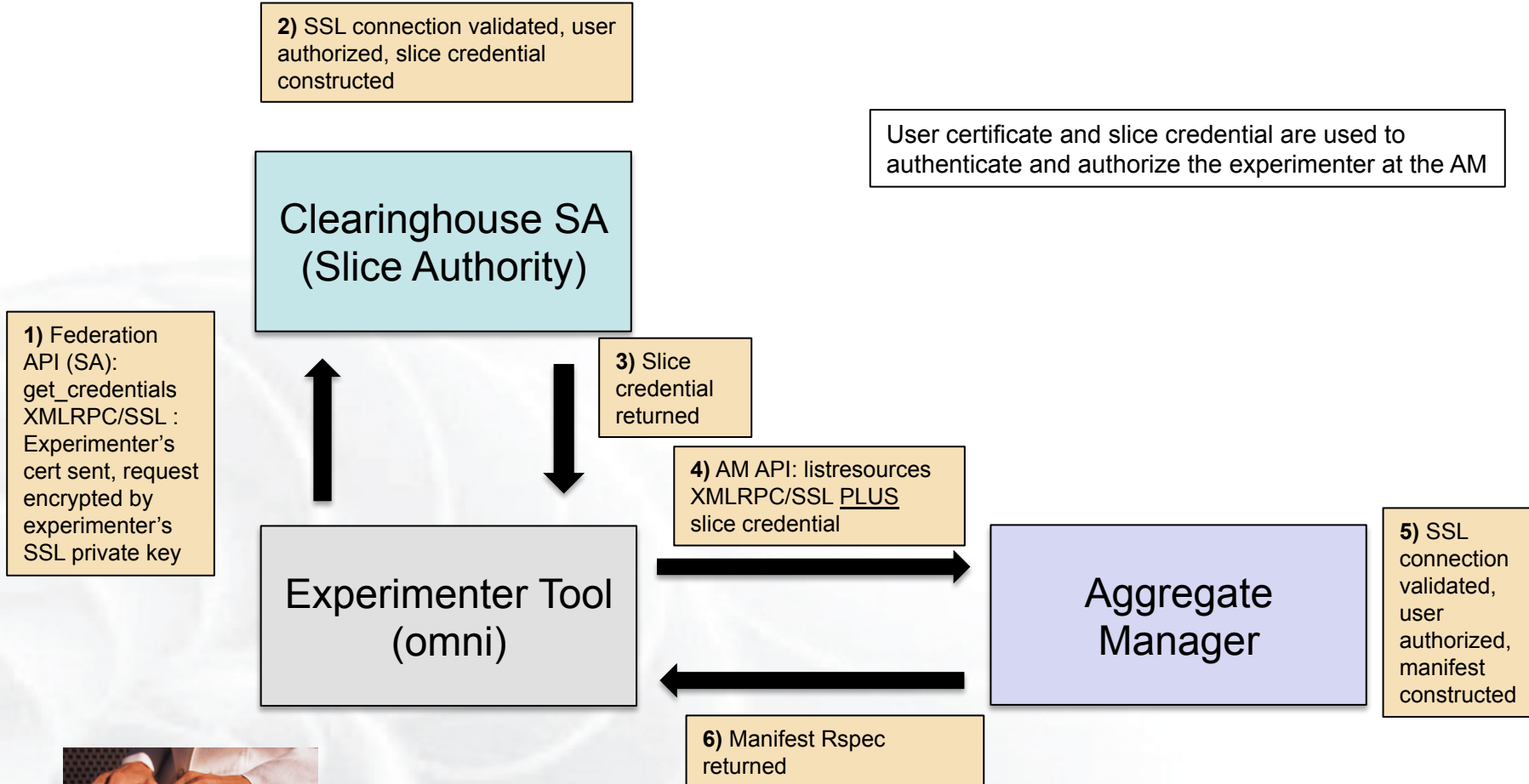
Resource Plane:
Racks, switches, PCs

Control Plane:
Aggregates [AM API],
Authorities [Federation API],
Tools, Slices, Slivers, Projects



This talk will focus on the entities comprising the GENI control plane and their relationships.

Architecture Schematic: Tools interacting with Aggregates



omni.py -a test-agg listresources myslice

What is a Slice Authority?



Why do I need to go from the Tool to the Slice Authority when I really want to go straight to the Aggregate?

What are all these Credentials and Certificates for?

I just want some resources!

GENI: Trying to give Experimenters the Resources they Need



Experimenter



Resource Owner

Who is this guy?

What should I allow him to have?

What happens if something goes wrong?

- “Who is this guy?”: **Authentication**
 - We need to know that the person asking for resources is who they claim to be.
- “What should I allow him to have?”: **Authorization**
 - We need to be able to determine which users are entitled to which resources in which context.
- “What happens if something goes wrong?”: **Accountability**
 - We need to be able to tell when an experiment is behaving in a way that risks my resources, and if so, shut it down and keep it from happening it again.

Providing experimenters with authenticated, authorized, accountable access to resources is the foundation of the GENI architecture.

Wanted: A Trusted Third Party

In general, the experimenter and the resource owner don't know each other and don't trust each other. Moreover, requiring that they do **won't scale** to large numbers of users and resources.

- For the resource owner to be willing to allocate resources to the experimenter, a mutually trusted third party is needed who can:
 - Vouch for the experimenter's identity
 - Provide information about the experimenter from which to make authorization decisions
 - Monitor experiments, provide alert, shutdown and forensics services, revoke privileges when needed

These trusted third parties are the Slice and Member Authorities

Participants in a GENI Federation

Federation: A collection of people and institutions who agree to share resources and abide by common procedures in order to share resources in a reliable, mutually beneficial manner.

Clearinghouse: Set of services establishing federation-level authentication, authorization and accountability of experimenter use of federation resources. Esp. contains one or more Slice Authorities and Member Authorities

Monitoring: Processes and tools monitoring activity on GENI resources for health, performance, adherence to policies.

Tools: Software capabilities that interact with federation resources on behalf of experimenters

Aggregates: Software entities that represent federated resources in transactions with experimenter tools.

Experimenter: A researcher seeking to perform network experiments on customized data plane.

Resources: Physical resources (compute, network, storage) made available to the federation by means of a participating aggregate.



Real-world entities



Software entities

A **credential** is a signed statement.

In GENI, we have many different kinds of credentials that are used in different ways

- A **Certificate** is an *identity* credential:
 - “The person bearing the private key associated with this public key has these attributes: UUID, URN, email...”
 - In GENI, these are in X509 format, signed by a Federation Member Authority.
- Certificates are the basis of **Authentication** in GENI.
 - All API calls (to aggregates through the AM API or to the Clearinghouse through the Federation API) are made via SSL using the caller’s certificate and private key

- Slice and User Credentials
 - Slice credentials are statements from the SA regarding rights and roles of a user with respect to a given slice
 - User credentials are statements from the MA regarding rights and roles of a user independent of a slice
 - The aggregate uses these to inform its own ***Authorization*** decisions
- Attributes
 - Statements about a user: “User is ...” a Project Lead or Operator or Faculty at X institute...
 - *These may be things that are true outside of GENI or within GENI*

- **Speaks-for Credentials**
 - Agent: “I grant this tool (or user) to speak on my behalf.”
 - Actor: “I am acting on your behalf”
 - And YOU are accountable
- **Delegation Credentials**
 - Agent: “I grant a particular right/privilege of mine to this other user”
 - Actor: “I am acting with your blessing”
 - And I am accountable

The Authorization Pipeline

Authentication



Identity



Attributes



Policy



Rights



Authorization

Authentication: An API (AM or Federation) call is made using user's certificate and private key. If the public key in cert matches private key, user is authenticated.

Identity: The caller's certificate contains some key identity attributes: URN, UUID, email.

Attributes: The call may contain other credentials (e.g. slice credential or PI attribute).

Policy: The server (SA, MA, AM) has rules determining what attributes are required to allow actions in a given context (e.g. slice).

Rights: Attributes crossed with policies leads to a specific set of rights in a given context.

Authorization: The call is (or is not) authorized if user has sufficient rights based on policy.

GENI does not apply independent reasoning to authorization: all the logic is in attributes and policies.

The elements of GENI (users, tools, federation services, aggregates) have different degrees of *trust* that allow them to interoperate

- We *mean* different things by ‘trust’, and represent them differently in the GENI architecture
 - **CREDIBILITY**: *If you claim it, I believe it*
 - Accepting your statements as true
 - Incorporation of your root cert into my ‘trusted root bundle’
 - **ENDORSEMENT**: *I vouch for you to others*
 - Directory services, membership, credential granting
 - **RELIANCE**: *I believe you can do something as I would want it done*
 - Delegation or Speaks-for credentials
 - *Implied* in using a tool, connecting to a service

Who trusts whom? What relationships are privileged?

Trusted entity

	USER	TOOL	CH	AM
USER		Reliance	Reliance	
TOOL		Reliance		
CH	Endorsement			Endorsement
AM			Credibility	

Trusting entity

We will review these different trust relationships, which may be represented and supported in different ways in the architecture.

Trust Relationships: CH trusts User

This is an ENDORSEMENT relationship

- The members of the Federation vet prospective members to validate their credentials and identity
- If validated, a Federation Member Authority mints an SSL certificate for that user:
 - Attests that the bearer of corresponding SSL private key has particular identity attributes (URN, UUID, email)

This cert allows access to GENI services and represents a statement of trust of the federation in this person.

If that trust is broken, the certs can be not renewed when expired, or [future] revoked.

GENI Account Activation Page

In order to activate your GENI account, you must first agree to GENI policies:

- [GENI resource Recommended Use Policy](#): GENI participants must follow these guidelines in using resources.
- **Ethics**: Be respectful of other GENI experimenters - these are shared resources.
- [Privacy](#): Some personal information, including that provided from InCommon, may be shared among GENI operators.
- **Cite GENI**: If you use GENI in your research or classroom, you must say so in your published papers or other documents. You may make this acknowledgement by citing the following paper: [GENI: A federated testbed for innovative network experiments](#). This [BibTeX entry](#) may be used to cite GENI.

If you send us a citation for your paper, we'll include it in the [GENI Bibliography](#).

You must also acknowledge that the GENI Clearinghouse and experimenter portal are currently in a beta release stage. There are bugs and missing features. Let us know, and we will try to address the issues.

I agree to the GENI policies.

If authorized to do so, the GENI portal can help you reserve and manage GENI resources, and is recommended for most GENI users.

I authorize the GENI Portal to act on my behalf in GENI.

This is a CREDIBILITY trust relationship

- The act of an aggregate joining a federation is the inclusion of the root certificate of that federation in its trusted set
 - Connections to the aggregate are validated against the trusted set and only connections that can be resolved to one of the trusted roots will be accepted
 - Slice Credentials and User Certificates Credentials are validated against the same trusted set
 - *“If the MA trusts this user or the SA validates the user’s rights at a slice, I will too”*
 - Aggregates can be members of multiple federations by including each federation’s root certificate in its trusted set

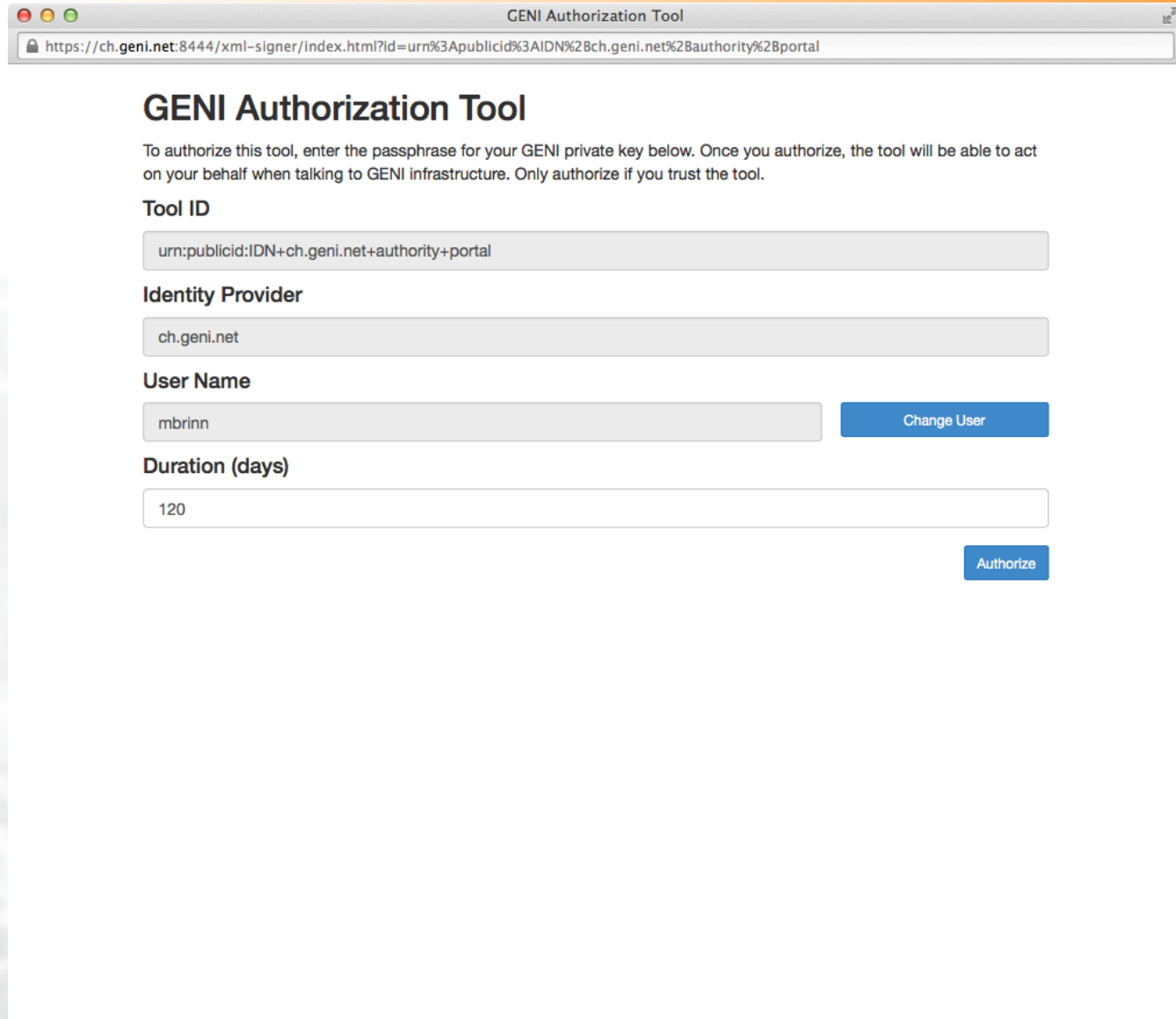
- Members of the federation trust AMs in that they vet them for proper operations and capable management and vouch for them
 - Advertising them in the Federation Service Registry
- Users do not, themselves, need to trust the aggregates: they can rely on the endorsements of the CH

GENI limits the number of trust relationships required to allow reliable resource sharing from $M*N$ to $M+N$ (where M is the number of users and N is the number of aggregates)

- In GENI, we distinguish two classes of tools
 - **Desktop**: These tools ‘speak as’ the user using the user’s cert/key and runs under the user’s control.
 - Example: omni
 - Run on user’s own computer: key never leaves machine.
 - **Hosted**: These ‘speak as’ themselves using their own cert/key and ‘speak for’ the user using a speaks-for credential.
 - Example: GENI Portal
- A speaks-for credential is a statement signed by the user that they authorize the tool to speak on the user’s behalf.

This is a RELIANCE trust relationship

Trust Relationships: User trusts Tool



The screenshot shows a web browser window titled "GENI Authorization Tool". The address bar contains the URL: `https://ch.geni.net:8444/xml-signer/index.html?id=urn%3Apublicid%3AIDN%2Bch.geni.net%2Bauthority%2Bportal`. The page content includes:

- GENI Authorization Tool**
- Instructional text: "To authorize this tool, enter the passphrase for your GENI private key below. Once you authorize, the tool will be able to act on your behalf when talking to GENI infrastructure. Only authorize if you trust the tool."
- Tool ID** field with value: `urn:publicid:IDN+ch.geni.net+authority+portal`
- Identity Provider** field with value: `ch.geni.net`
- User Name** field with value: `mbrinn` and a **Change User** button.
- Duration (days)** field with value: `120` and an **Authorize** button.

Trust Relationships: User trusts CH

This is a RELIANCE trust relationship

- The trust a user has in the CH services is manifested in two ways:
 - Hosted tools will tend to validate the CH service's cert much as the CH validates the user's cert
 - This giving users the assurance of correct HTTPS authentication
 - By directing tools to interact with the CH services (Slice Authority, Member Authority, Service Registry) the user is trusting their correct function



omni_config:

Omni AM API call:

```
python omni.py -V2 -a https://130.127.88.98:5002 listresources ONETWOTHREE
09:27:50 INFO omni: Loading agg_nick_cache file '/Users/mbrinn/.gcf/agg_nick_cache'
09:27:50 INFO omni: Loading config file /Users/mbrinn/.gcf/omni_config
09:27:50 INFO omni: Using control framework chapi
09:27:50 INFO omni: Member Authority is https://ch.geni.net/MA (from config)
```

```
[omni]
default_cf=chapi
users=mbrinn
default_project=COUNT
```

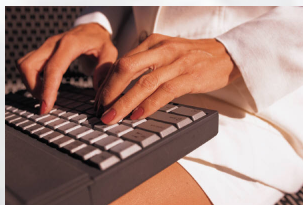
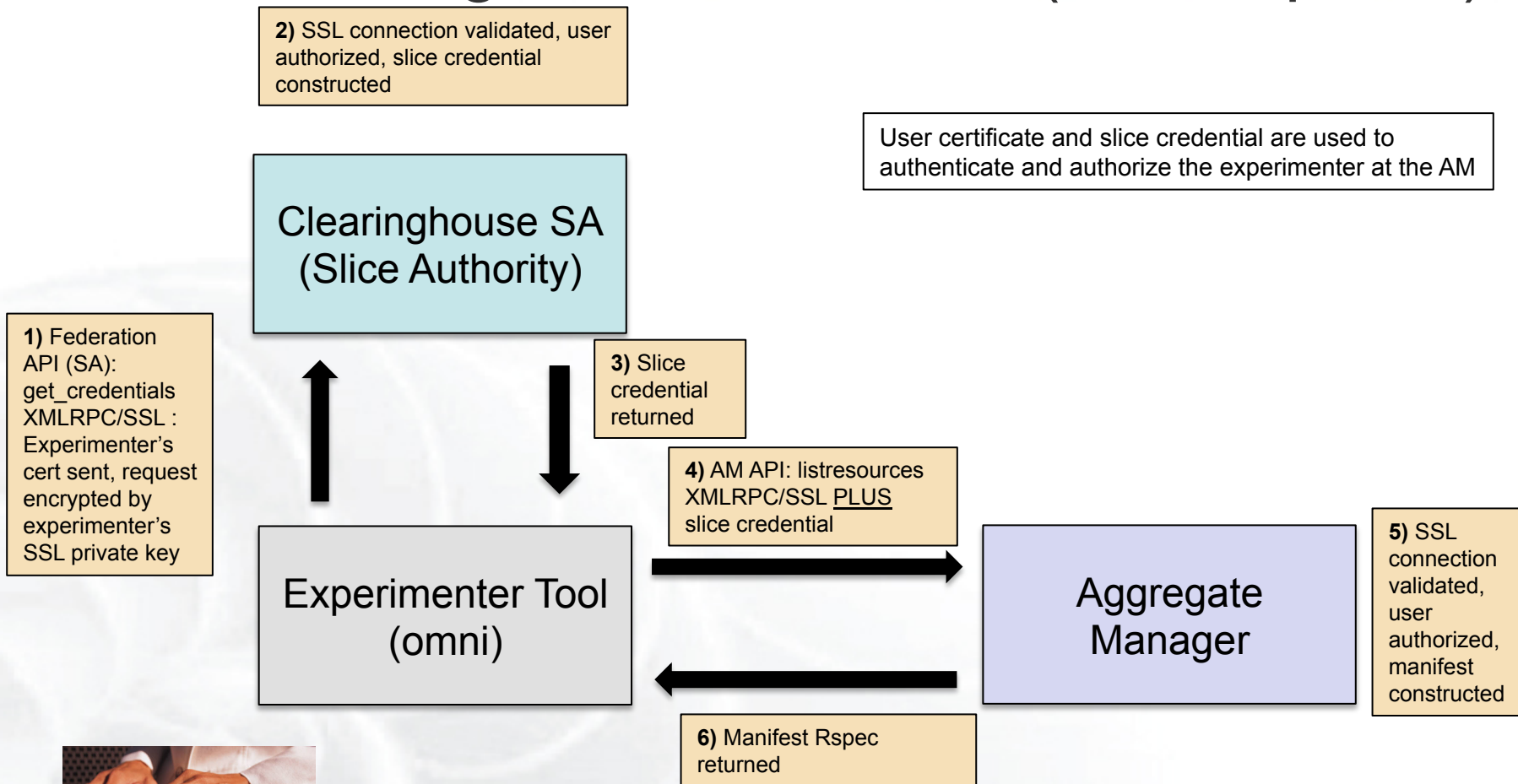
```
[ [chapi]
speakv2 = True
type = chapi
authority = ch.geni.net
ch = https://ch.geni.net:8444/SR
sa = https://ch.geni.net/SA
ma = https://ch.geni.net/MA
cert = /Users/mbrinn/chapi_scaling/pems-nye/mbrinn-cert.pem
key = /Users/mbrinn/chapi_scaling/pems-nye/mbrinn-key.pem
```

HREE expires on 2014-06-17 11:48:12 UTC

Result Summary: Queried resources for slice ONETWOTHREE from 1 of 1 aggregate(s).

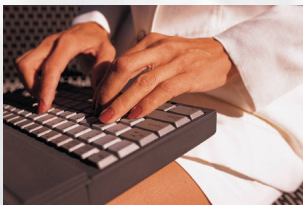
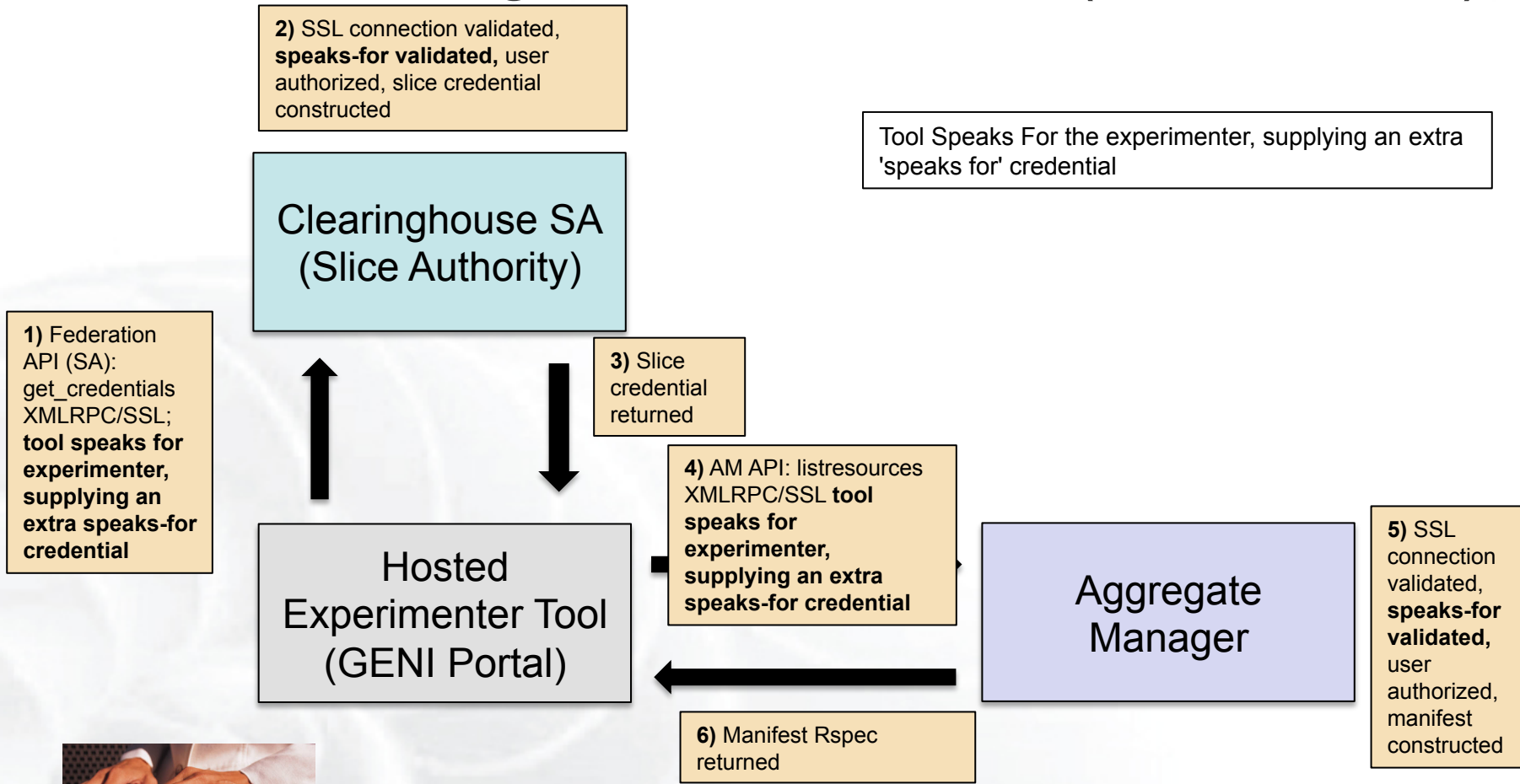
```
09:27:51 INFO omni: =====
```

Trust Credentials at work: Getting a slice manifest (Desktop tool)



omni.py -a test-agg listresources myslice

Trust Credentials at work: Getting a slice manifest (Hosted tool)

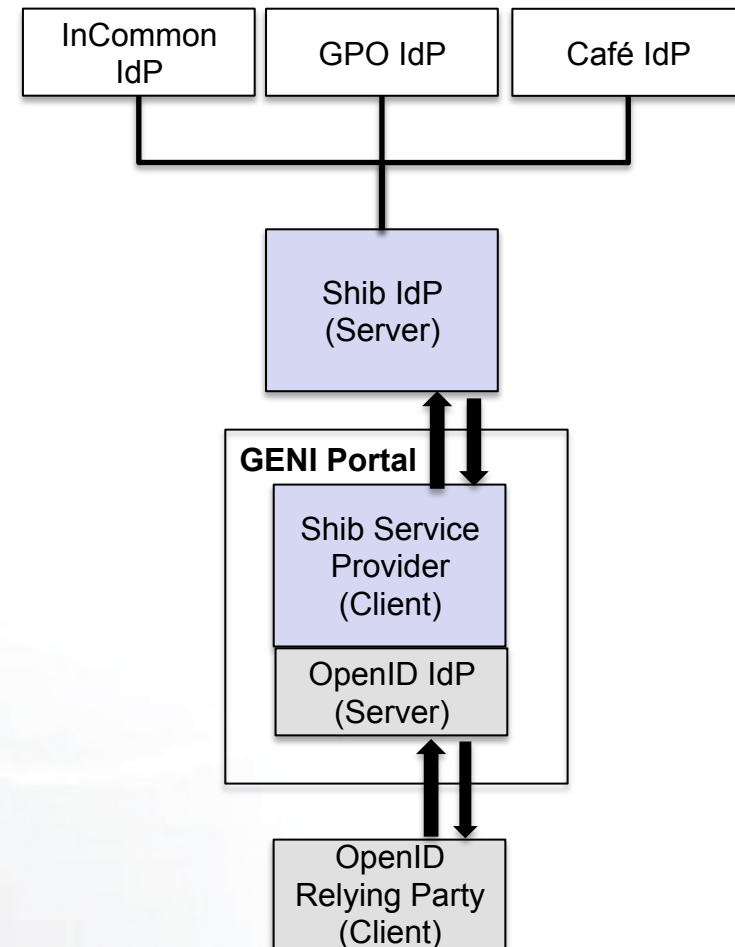


GENI Slice: *myslice*



This is a RELIANCE trust relationship

- The GENI Portal serves as
 - A Shibboleth Service Provider (i.e. client to the Shib IdP)
 - An IdP for OpenID clients (e.g. GEE, LabWiki, WiMAX)
- The tools who use the Portal's OpenID IdP trust the Portal to authenticate users properly and return their attributes.

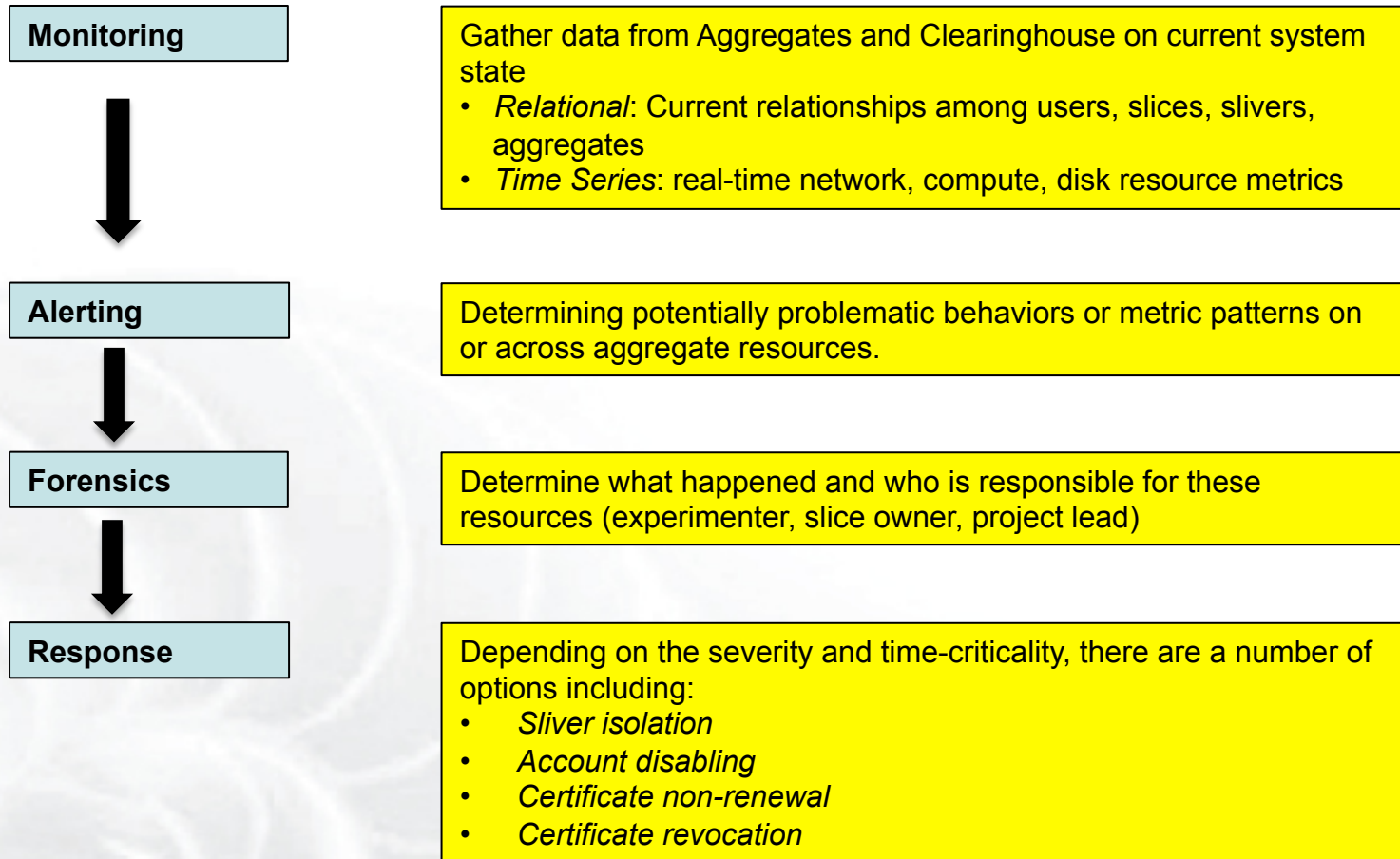


GENI Portal OpenID Trust

You are about to release some of your information to <http://igplc.cs.princeton.edu:8080/>.

Do you trust <http://igplc.cs.princeton.edu:8080/>?

GENI Accountability Foundations



GENI has a variety of processes, policies and procedures that ensure that experimenters can, if necessary, be accountable for actions taken on federation resources

- GENI seeks to build a trusted environment in which experimenters and resource owners can participate in resource allocation
 - These trust relationships reflect human/inter-organizational relationships, nothing more.
- Authentication, Authorization, Accountability are the pillars of that trust
- Credentials and Policies are the critical enablers of these pillars.

Questions?

- help@geni.net
- mbrinn@bbn.com