Issues in the Multiple Uses of Federation with GENI
Dr. Ken Klingenstein

The federated paradigm, implemented in modern technologies first in the identity management space, is an attractive model for many other problem areas. It offers local autonomy in many of the implementation choices, but creates a global service capability through the "narrow waist" of federated policies, shared attributes, and technology interfaces it operates under.

Federated identity has been a remarkable success. Based on SAML and a rich set of metadata, as embodied in software such as Shibboleth and simpleSAML.php, it has resulted in the formation of extensive R&E identity federations in over 25 major countries, spanning over 100 million users. It has gained strong traction in government and now in business, with vertical sectors beginning to develop federations. As the SAML assertions can contain attributes as well as identity, or instead of identity, identity federations provide the rudiments of authorization as well. And, though less deployed, XACML, a companion language to SAML, allows rich expression of authorization policies to turn the identity attributes into authorization decisions.

Moving from federated identity to federated resources (denoted as federated *) raises several key issues:

Reconciling the different perimeters of federated * - Each of the categories of federation under discussion within GENI will federate along their own "natural" boundaries. Routers might federate at the autonomous system level; computing resources might federate at a sysadmin or agency level; file systems might federate at a namespace level; users federate at an organizational and national sector levels; search federates across licenses signed by organizations. None of those acts of federation will be trivial - much needs to be negotiated and then, once agreed on, actively managed. Moreover, at the identity federation level, several relationships can exist among autonomous federations, including interfederation, confederation, and soup. How these relationships apply to the rest of federated * is unknown at this point and compound the perimeter issues. To the degree that requirements cross-cut federations with different perimeters, all issues become far more complicated.

Use of emergent interfederation technologies to address cross-boundary issues – Within the identity federation space, an essential protocol (MDX – MetaData Exchange) is now being implemented to address the metadata issues in identity interfederation. MDX is a powerful and scalable tool, closely paralleling the dns/routing approaches of the Internet. Its value to address interfederation between things in federated * is unknown, but it may serve as a valuable tool.

Application of federated identity techniques and technologies to federated * - Identity federation is a proven success, and its approach to the fundamental issues of creating and managing federations seems canonical. Early work is now going on to see if approaches to federating GENI resources can use approaches that parallel

the identity approaches, with devices, aggregators, etc exchanging SAML assertions that contain attributes.

Addressing discovery – In identity federations, a particularly awkward issue exists in having an unauthenticated user indicate the realm they want to authenticate in. This "discovery" problem, as embodied in the various federation WAYF's currently, is likely not as severe in federated *.

Layering dynamic trust on top of static trust – While dynamic trust is attractive for its flexibility, the elements of federation - agreements, operational practices, the narrow waist interfaces, etc – do not happen spontaneously. Some of them, such as contracts, have long latencies. Dynamic trust may be best executed as a dynamic protocol riding on top of a relatively static trust fabric, or inter-federated fabrics. Figuring out both the static plane and the dynamic plane for the various federated * is an important part of the work going forward.

Requirements for attribute aggregation, LOA of attributes, scoping, etc. As identity and access control federations mature, new issues are emerging that can inform the initial conversations on federated *. The issues include the confidence in attribute value assignments, assertions by a third party, use of query languages, etc. It is likely that analogues of these issues will exist in federated *.

Managing metadata –the core of multilateral federations is the shared metadata exchanged by participants. It is dynamic both in the values within the metadata and the attributes that the federation chooses to exchange. It needs aggregation and dissemination mechanisms, as well as validation and certification by the federated operator.

Addressing transit issues – federated identity deals with two end-points – the IdP and the SP, and provides a hook for portals recently with new capabilities in delegation and aggregation. In the GENI context, and in the networked and distributed resources at the hardware layers, there are numerous transits – of networks, of intermediaries, etc. Can the federated identity approach be extended to work with transit use cases?

Coupling of identity and authorization – Identity federations also serve as access control federations, where access control is defined to be providing external attributes and entitlements for authorization decisions to be made by a resource. In some cases, the authorization is actually made at the IdP and an "entitlement" is conveyed in the assertion to the resource. This linkage of identity and access control needs to be reexamined in the other cases of authorization for federated *.