GEC22 OGF Meeting 2015

# A Federated Approach for Authentication and Authorization in the Network Services Framework

Carlos E. Rubio-Medrano and Gail-Joon Ahn

IRA A. FULTON SCHOOLS OF engineering ARIZONA STATE UNIVERSITY

sefcom security engineering for future computing

# Outline

- Requirements for *Authentication and Authorization* (A&A)
- Our Approach: a dedicated *attribute-based* NSI Service
- Revisiting A&A Requirements and Sample Policies

# Selected NSI A&A Requirements

| | ESnet | GEÁNT | NORDUnet |
|---|---|---|---|
| No end-to-end commercial traffic | ✓ | ✓ | ✓ |
| Commercial traffic allowed for research | ✓ | | |
| Resource access based on trusted identities | ✓ | ✓ | ✓ |
| NSI operators with overriding capabilities | ✓ | | |
| Net admins may override/deny access to sites | ✓ | ✓ | |
| Traffic allowed only between certain ends | ✓ | ✓ | ✓ |
| Traffic to US only for certain ends | | | ✓ |
| Resource access based on projects/groups | ✓ | | ✓ |
| Integration with protocol-specific policy formats | ✓ | ✓ | ✓ |

# Summary of NSI A&A Requirements

- Policy Management
  - Incorporate evaluation with service-specific functionality
  - Real-time data collection for policy evaluation
  - Evaluate/enforce both *local* and *inter-organizational* policies
- Authentication and Access Control
  - Support different models: identity-based, project/group-based and request-based
- Infrastructure
  - Leverage existing infrastructure
  - Scalability
  - Platform-independent

# Our Approach: Attributes

- Observable *security-relevant* properties attached to A&A *entities* (users, resources, etc.) either *natively*, e.g. innate characteristic, or *artificially*, e.g. username

- May be defined as 3-tuple: <*name, type, value*>*

- Examples: <username, String, "Carlos">, <port, Integer, 8080>, <bandwidth, Integer, 10>, etc.

*Rubio-Medrano, Carlos, Clinton D'Souza, and Gail-Joon Ahn. "Supporting secure collaborations with attribute-based access control." *IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom).* Austin, TX, USA: IEEE, 2013. 525-530

# Security Attributes

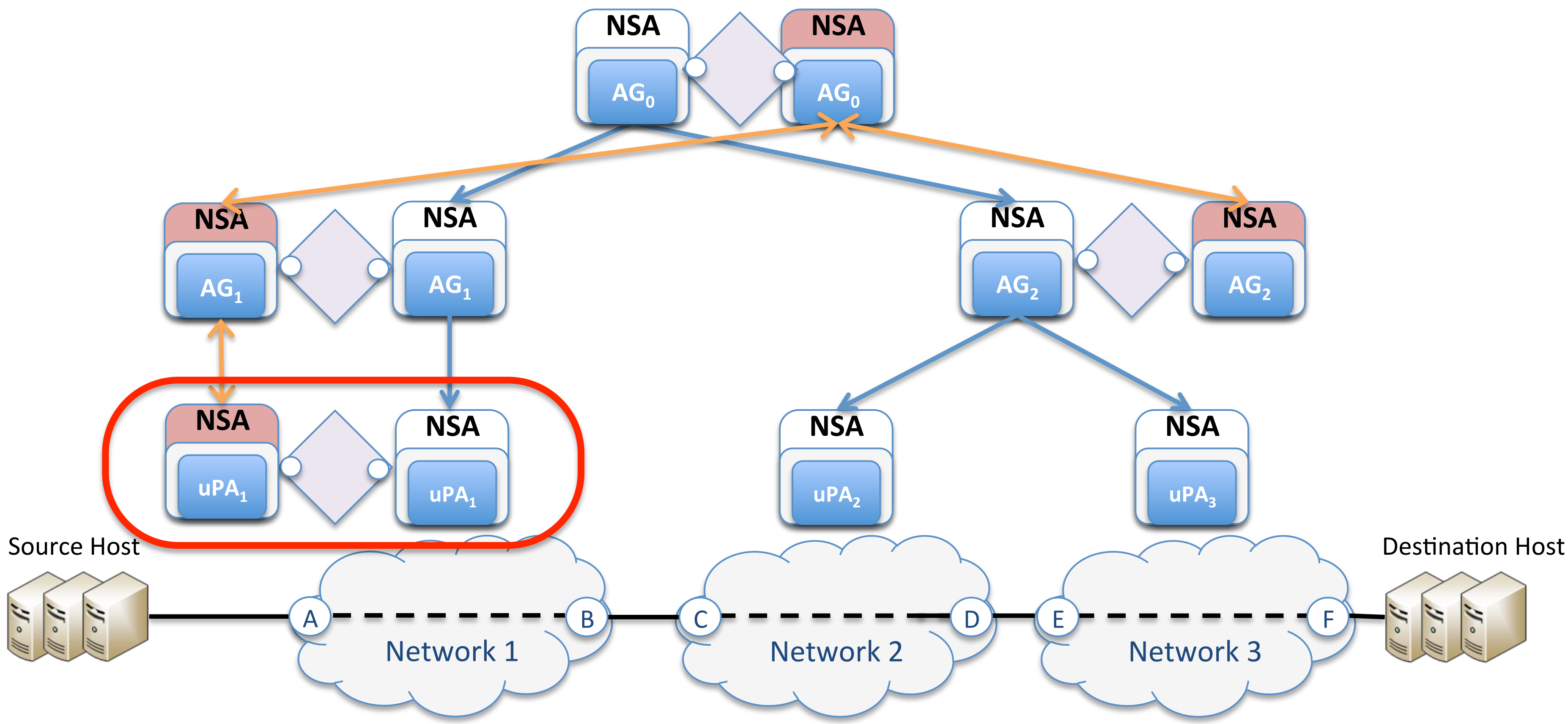
- A special case of *non-modifiable*, *fully-trusted* and possibly *custom-defined* attributes
- Provide a representation of *abstract* concepts such as
  - group memberships: <userGroup, Group, “CERN”>,
  - security states: <currentState, MachineState, “Safe”>,
  - roles: <userRole, Role, “Administrator”>,
  - access tokens: <token, AccessToken, “Link AX”>,
  - PKI identities: <userKey, PublicKey, “CarlosKey”>
  - Etc.
- May be *derived* from other attributes, either regular or security ones

# Our Approach: NSI Service

- We propose a *federation* for A&A based on *attributes*
- Dedicated NSI Service[1], implemented by NSAs[2] on top of each network, connected to other services through a*daptations*
- Manages definition, conflict resolution and distributed evaluation of A&A *policies* as well as the definition and provisioning of local and federated *attributes*

*1 Network Services Interface.* Roberts, Guy, et al. *Network Services Framework 2.0.* Grid Forum Document (GFD), 2014
*2 Network Service Agent.* MacAuley, John. *Network Service Agent Description Document.* Grid Working Document (GWD), 2014

# NSI A&A Service Adaptations



# Our Approach

- Policy Management:

  *Attributes:* Identify security-relevant properties from local resources or users that may serve as *attributes*

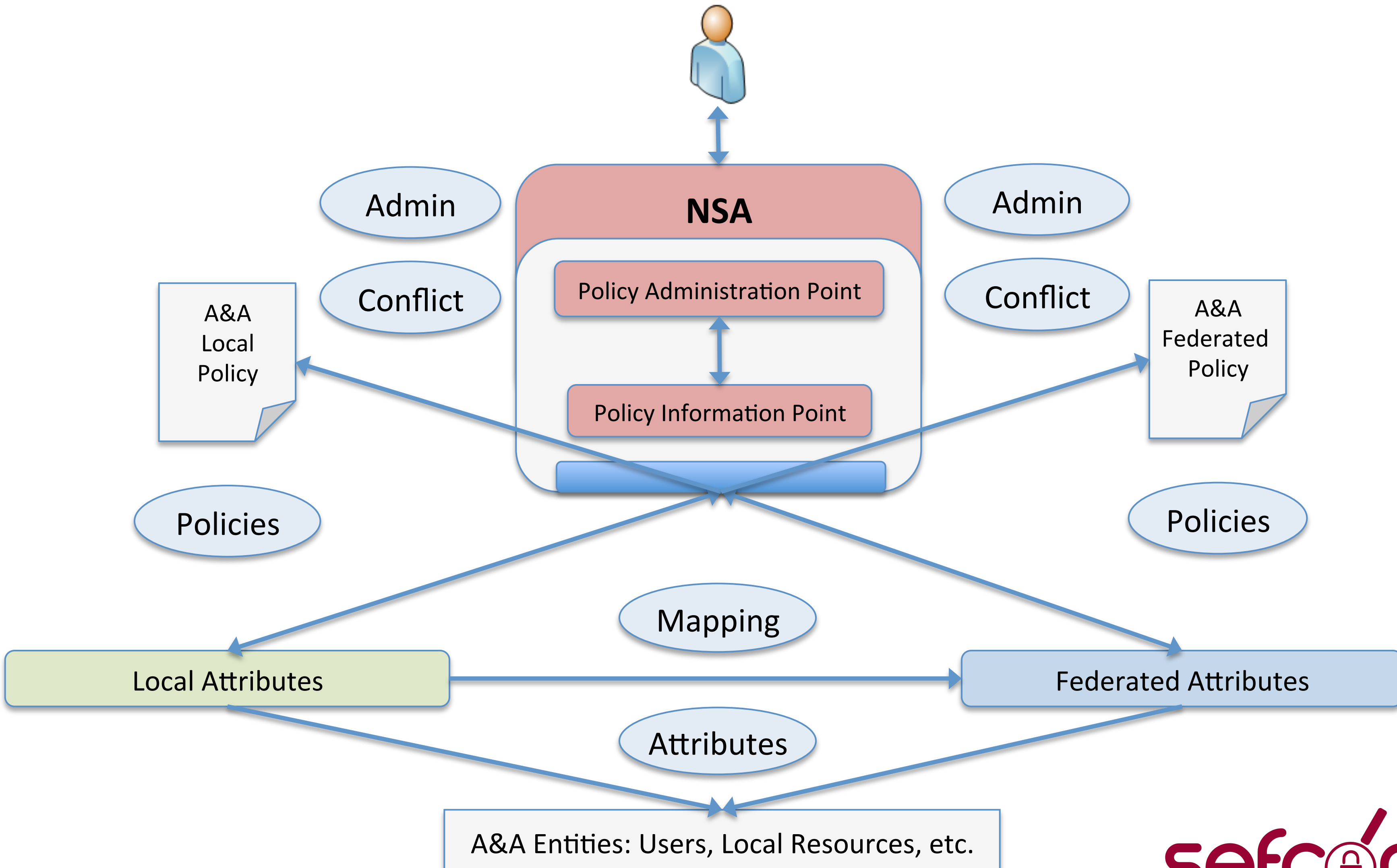
  *Mapping:* Map *local* attributes to *federated* attributes

  *Policies*: Allow for the *specification* and *discovery* of federated attributes for policy construction

  *Admin:* Allow for the *administration* (creation, update, removal) of both local and federated policies

  *Conflict:* Detect and help resolve policy conflicts, e.g., contradictory rules

# Our Approach



# Our Approach

- Policy Evaluation:

  *Retrieve:* Identify *relevant* local policies upon a given A&A request

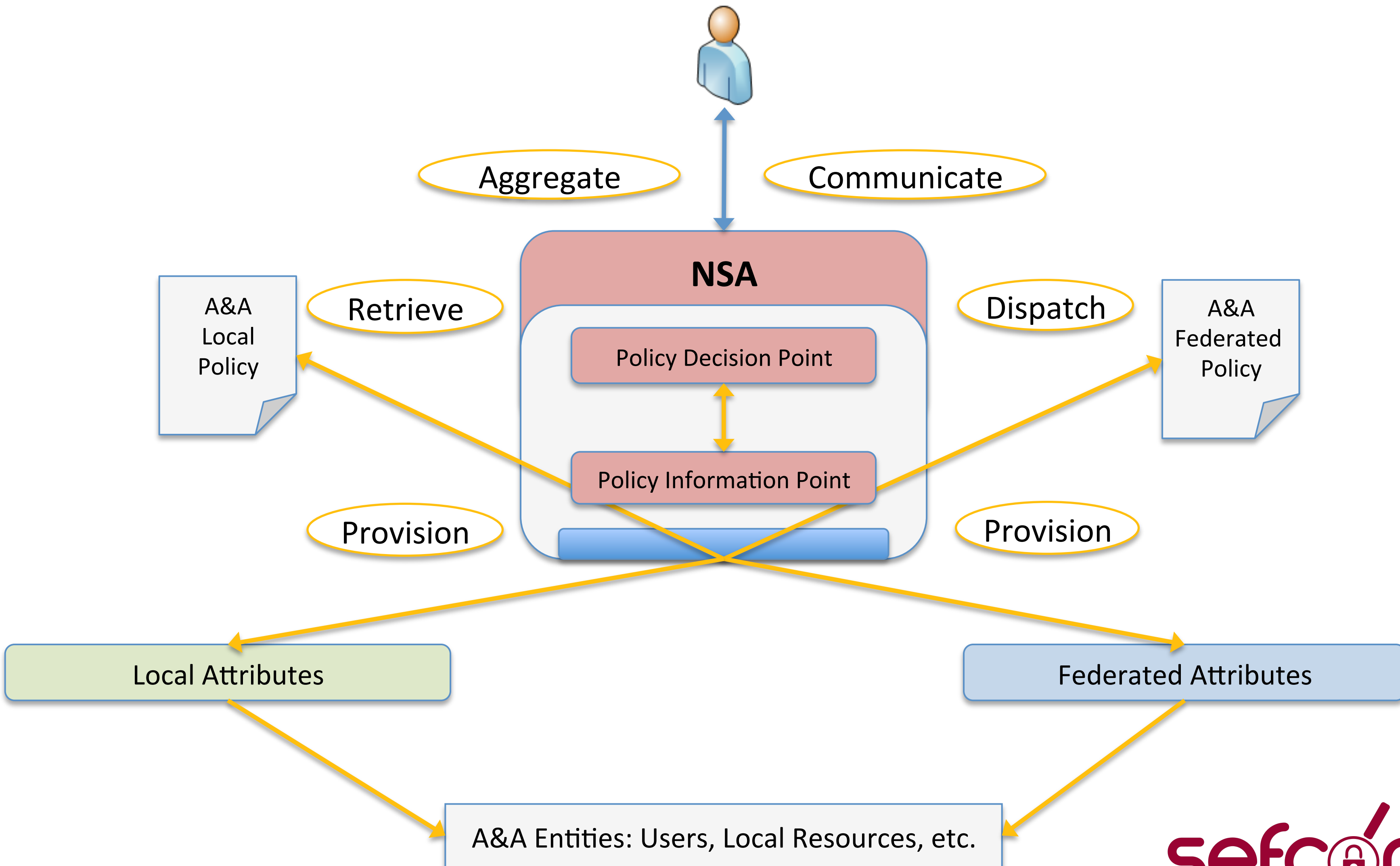
  *Provision:* Collect local and federated attributes as specified in relevant local policies

  *Dispatch:* Dispatch evaluation requests for relevant federated policies

  *Aggregate:* Combine evaluation decisions for both local/ federated policies

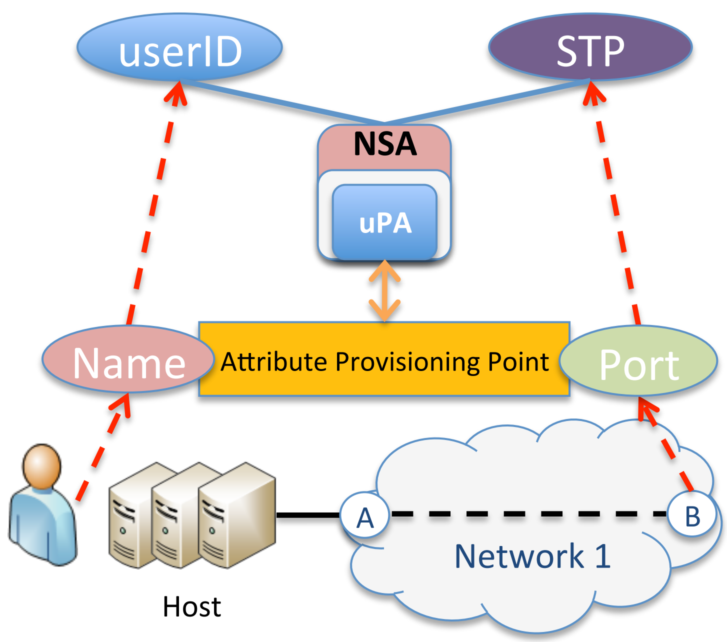
  *Communicate:* Send a response with the final A&A decision to the requesting service

# Our Approach



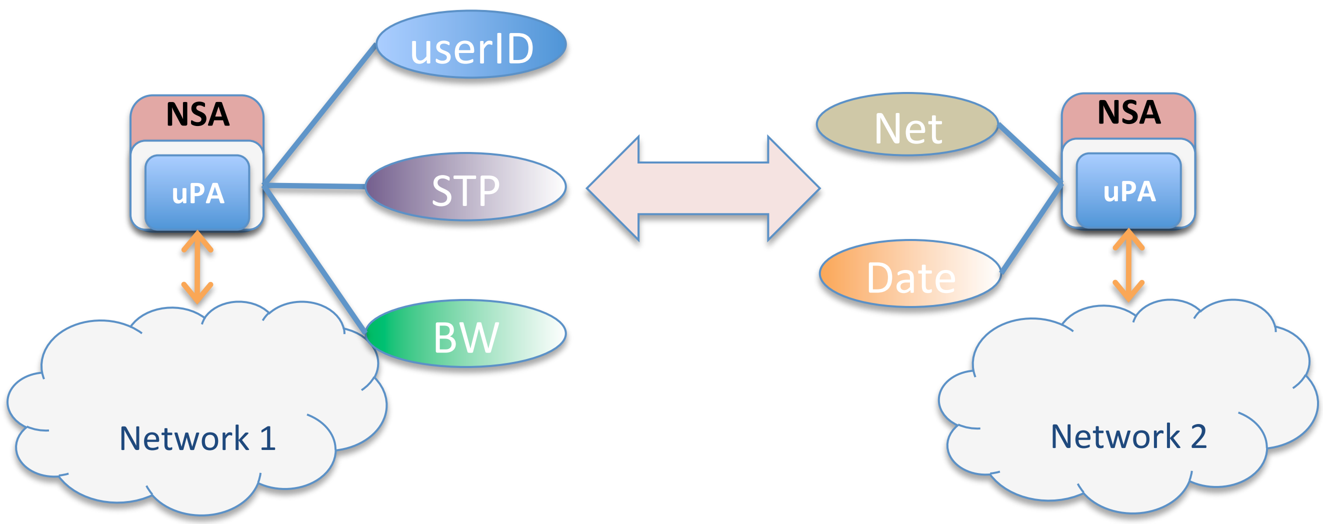
# Policy Management

1. *Identify policy-relevant properties from local resources or users that may serve as attributes*
2. *Map local attributes to federated ones*
   - Provide a framework for specifying and publishing both local and federated attributes



# Policy Management

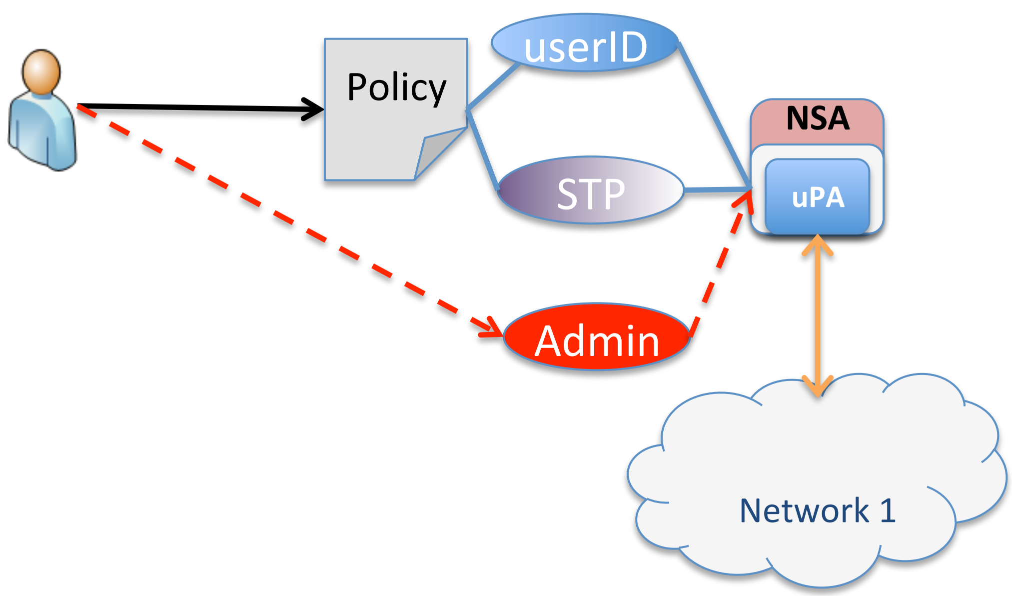
3. *Allow for the specification and discovery of federated attributes for policy construction*
    - Provide a distributed service that allows for the efficient discovery of federated attributes and policies within federated peers



# Policy Management

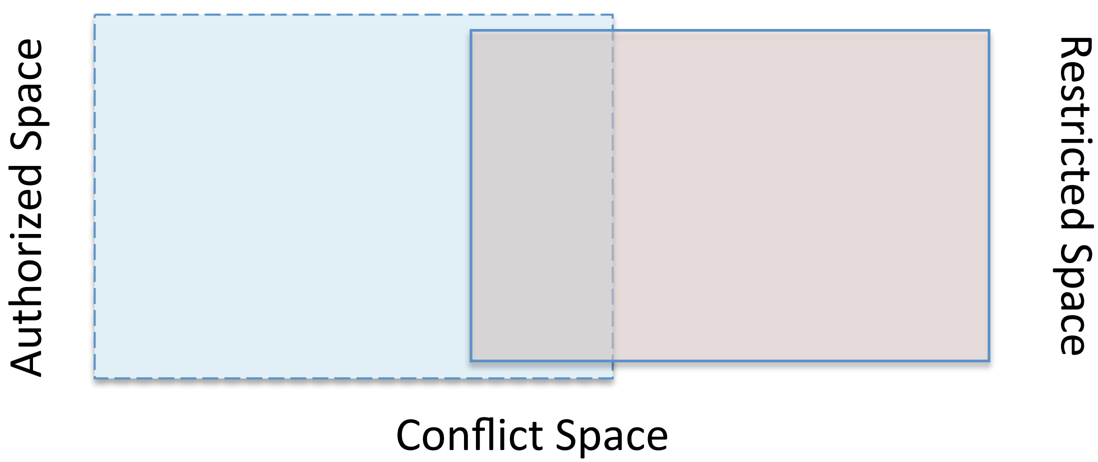
4. *Allow for the administration (creation, update, removal) of both local and federated policies*

   - Implement an A&A administration model based on *attributes*, allowing for certain users to create, update and remove attributes and policies only if they hold certain attributes, e.g. *network administrators*



# Policy Management

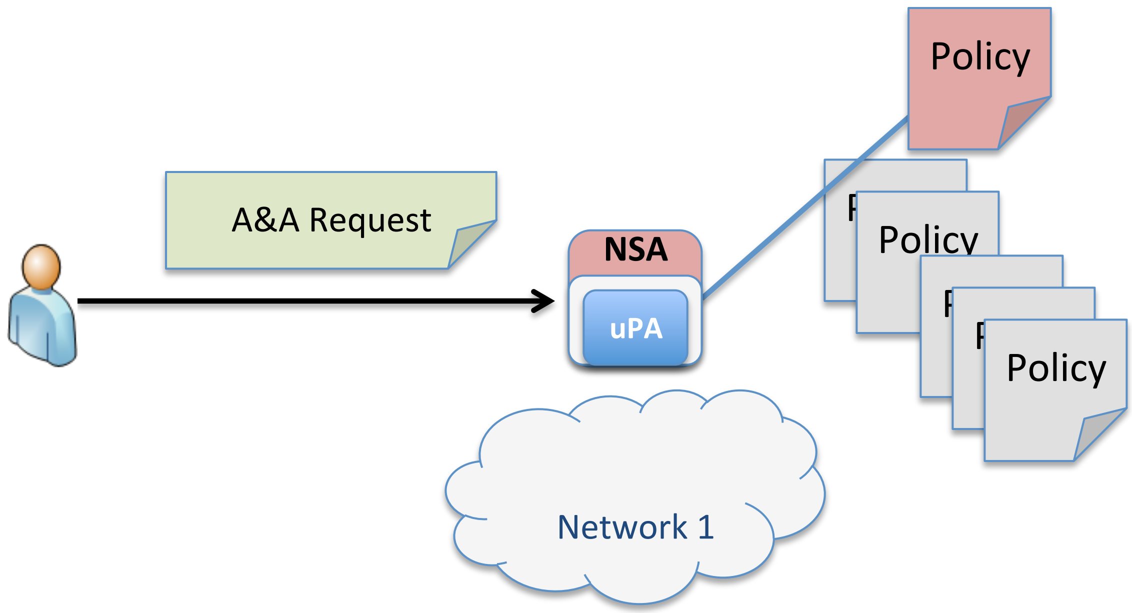
5. *Detect and help resolve policy conflicts, e.g., rule shadowing, generalization, correlation and redundancy.*
    - Develop new techniques that leverage existing approaches for conflict detection/resolution, e.g. *authorization spaces**, to work on a distributed multi-organizational setting




*Hu, Hongxin, Gail-Joon Ahn, and Ketan Kulkarni. "Detecting and Resolving Firewall Policy Anomalies." *IEEE Transactions on Dependable and Secure Computing* (IEEE) 9, no. 3 (May/June 2012): 318-331.

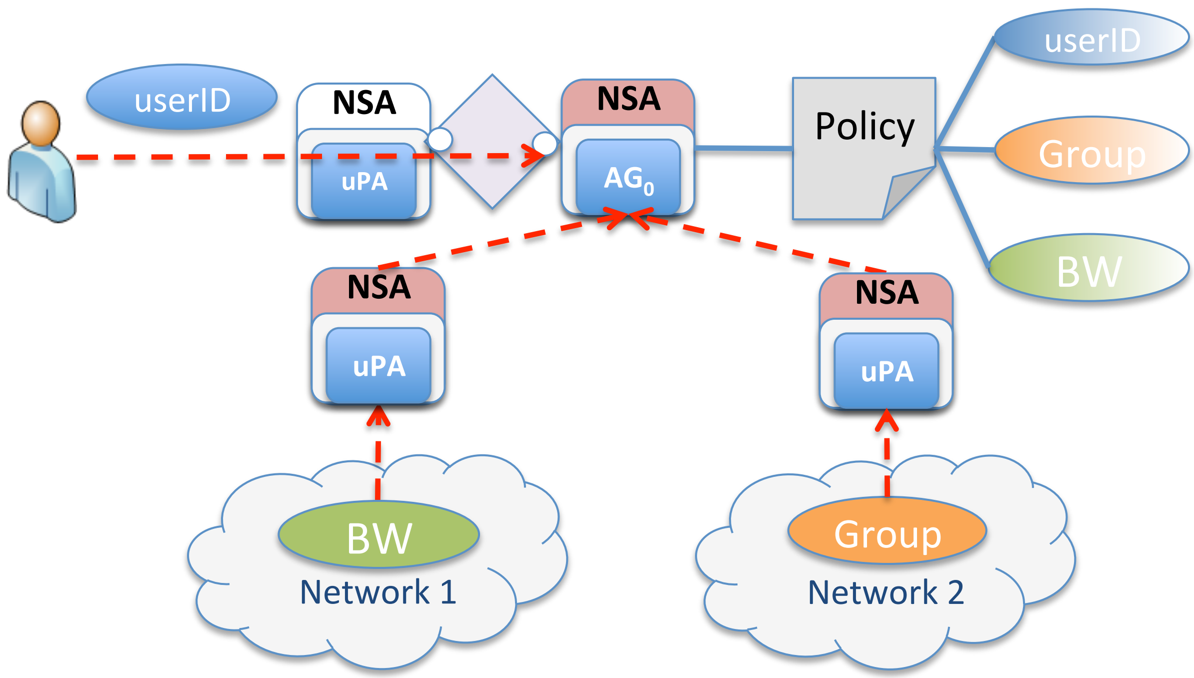
# Policy Evaluation

1. *Retrieve relevant local policies upon a given A&A request*
    - Develop policy indexing techniques to allow for relevant *local* policies to be efficiently located for evaluation



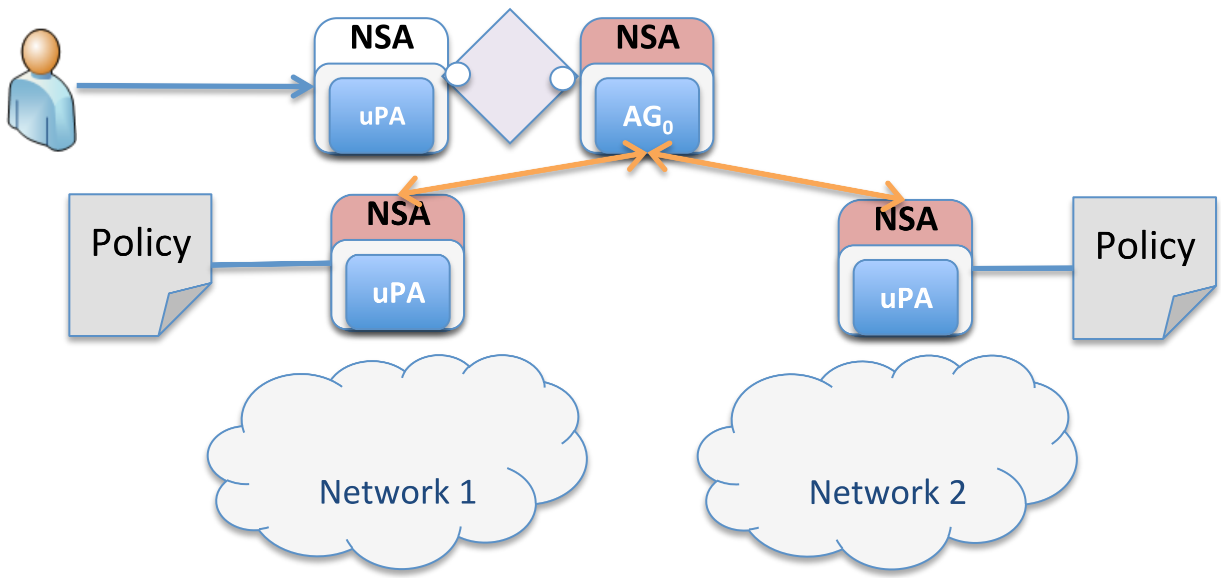
# Policy Evaluation

2. *Provision local/federated attributes as specified in relevant local policies*
   - Provide a framework for *provisioning*: processing, digitally signing and collecting both local and federated attributes that are relevant to a given policy



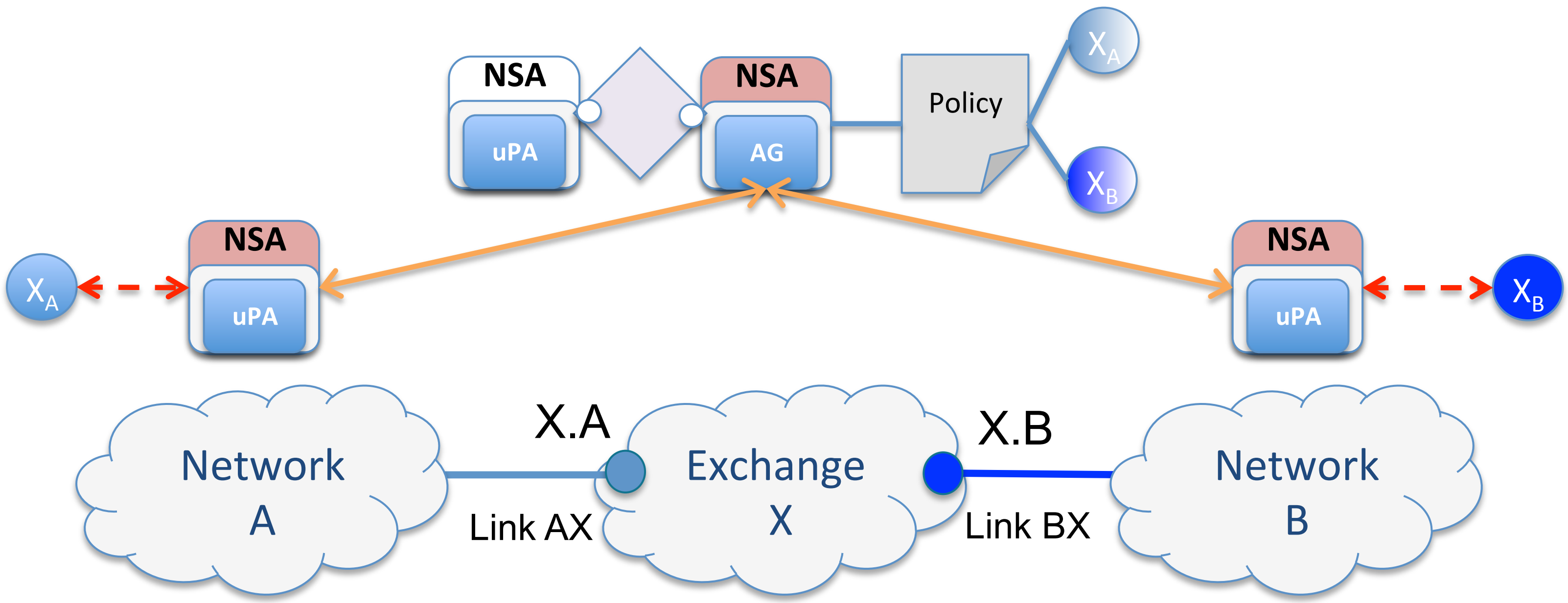
# Policy Evaluation

4. *Dispatch policy evaluation requests for relevant federated policies*
5. *Aggregate policy evaluation decisions for both local/federated policies*
6. *Communicate final A&A decision to requesting service*
    - Identify relevant A&A-NSAs using discovery service. Dispatch policy evaluation requests and aggregate results



# Policy Samples: Link Ownership

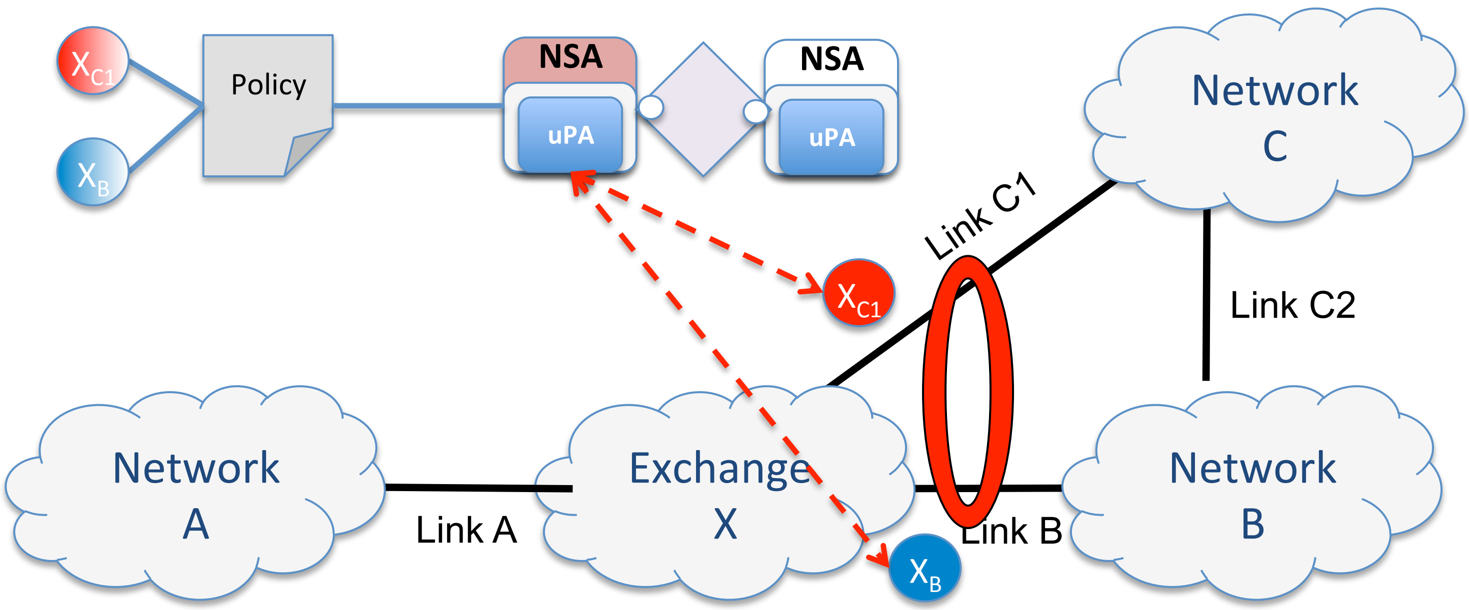
Exchange Network X cannot make a connection on port X.A without the approval of Network A, and similarly, cannot make a connection on port X.B without approval of Network B.



# Policy Samples: Resource Restrictive Transit

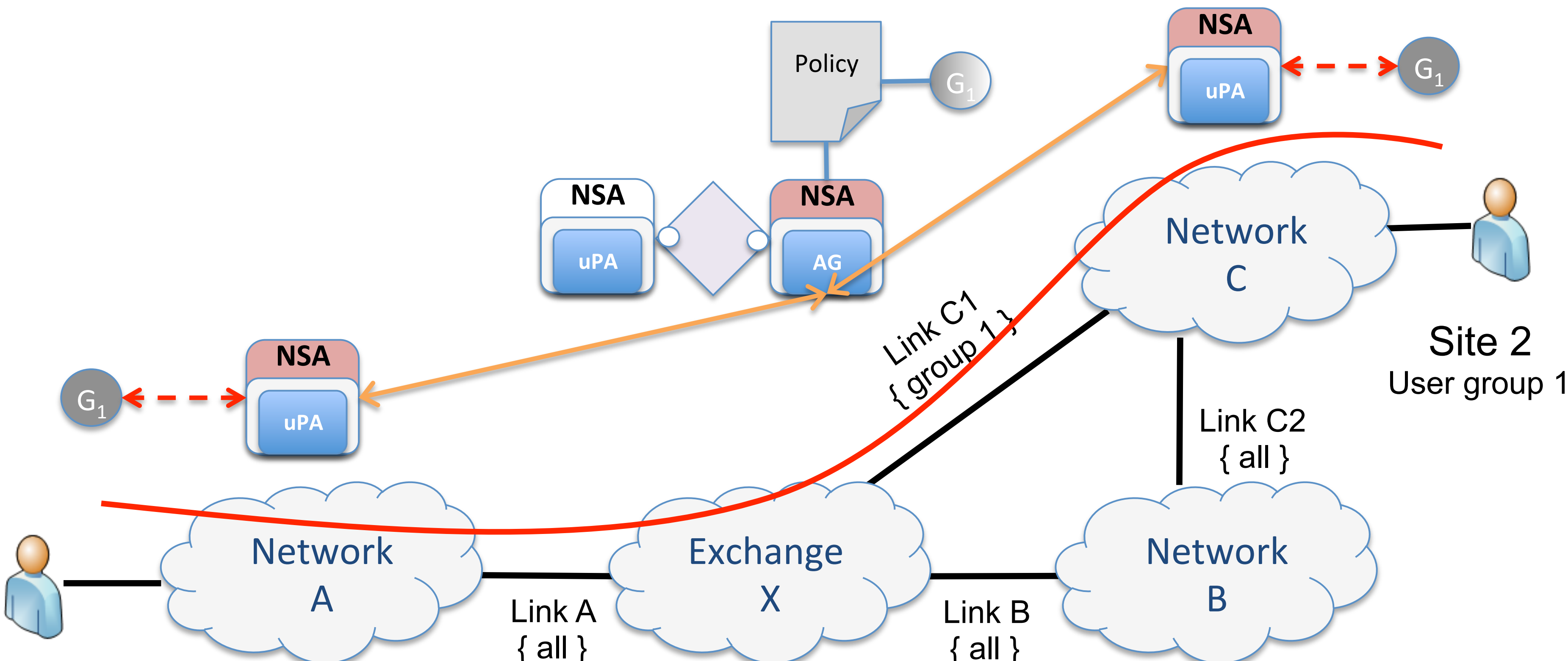
An example of a resource based transit policy is Exchange X allowing a maximum bandwidth between Network A and Network C independent of the path.

*Maximum bandwidth Link C1 + Link B for src Network C == 10 Gb/s*



# Policy Samples: Resource Allocation

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.



# Addressing NSI A&A Requirements

- Policy Management
  - Incorporate evaluation with service-specific functionality ✓
  - Real-time data collection for policy evaluation ✓
  - Evaluate/enforce both *local* and *inter-organizational* policies ✓
- Authentication and Access Control
  - Support different models: identity-based, project/group-based and request-based ✓
- Infrastructure
  - Leverage existing infrastructure ✓
  - Scalability ✓
  - Platform-independent ✓

# Questions?

- SEFCOM:
  - Website: http://sefcom.asu.edu

- Carlos Rubio-Medrano:
  - crubiome@asu.edu
  - http://www.public.asu.edu/~crubiome

- Gail-Joon Ahn:
  - gahn@asu.edu
  - http://www.public.asu.edu/~gahn1