

TeraGrid & GridShib

Tom Barton

University of Chicago

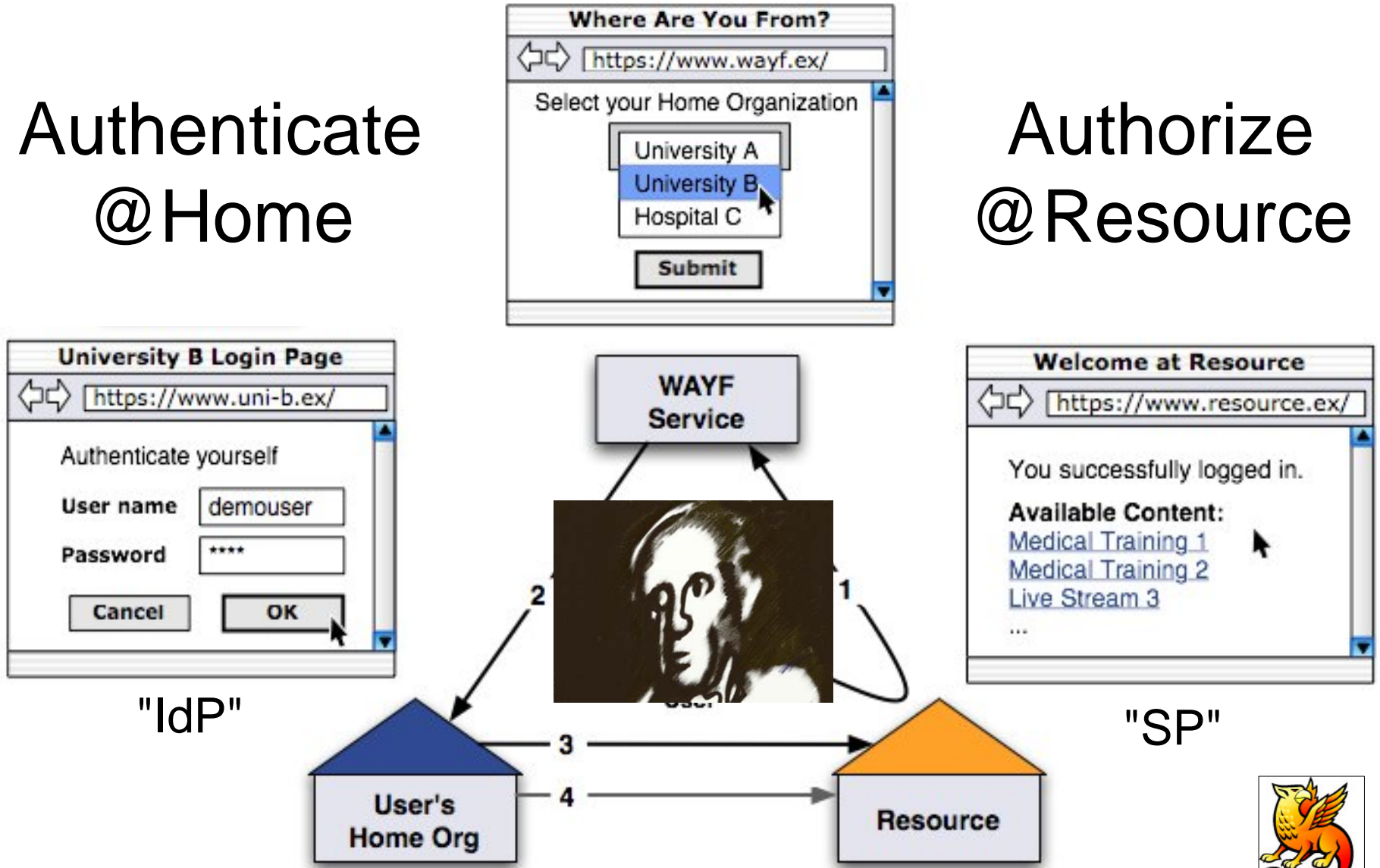
Scaling TeraGrid Usership



Approach to scaling problem: Federated Identity

Authenticate @Home

Authorize @Resource



"IdP"

"SP"

Federated Identity



ala Shibboleth

InCommon Federation

- Trust fabric: Metadata so that IdP's & SP's can mutually authenticate & interoperate
- Multilateral agreement among federation participants
 - Agree to actually operate as they claim to
- A “Where Are You From Service” available

TeraGrid Joining InCommon

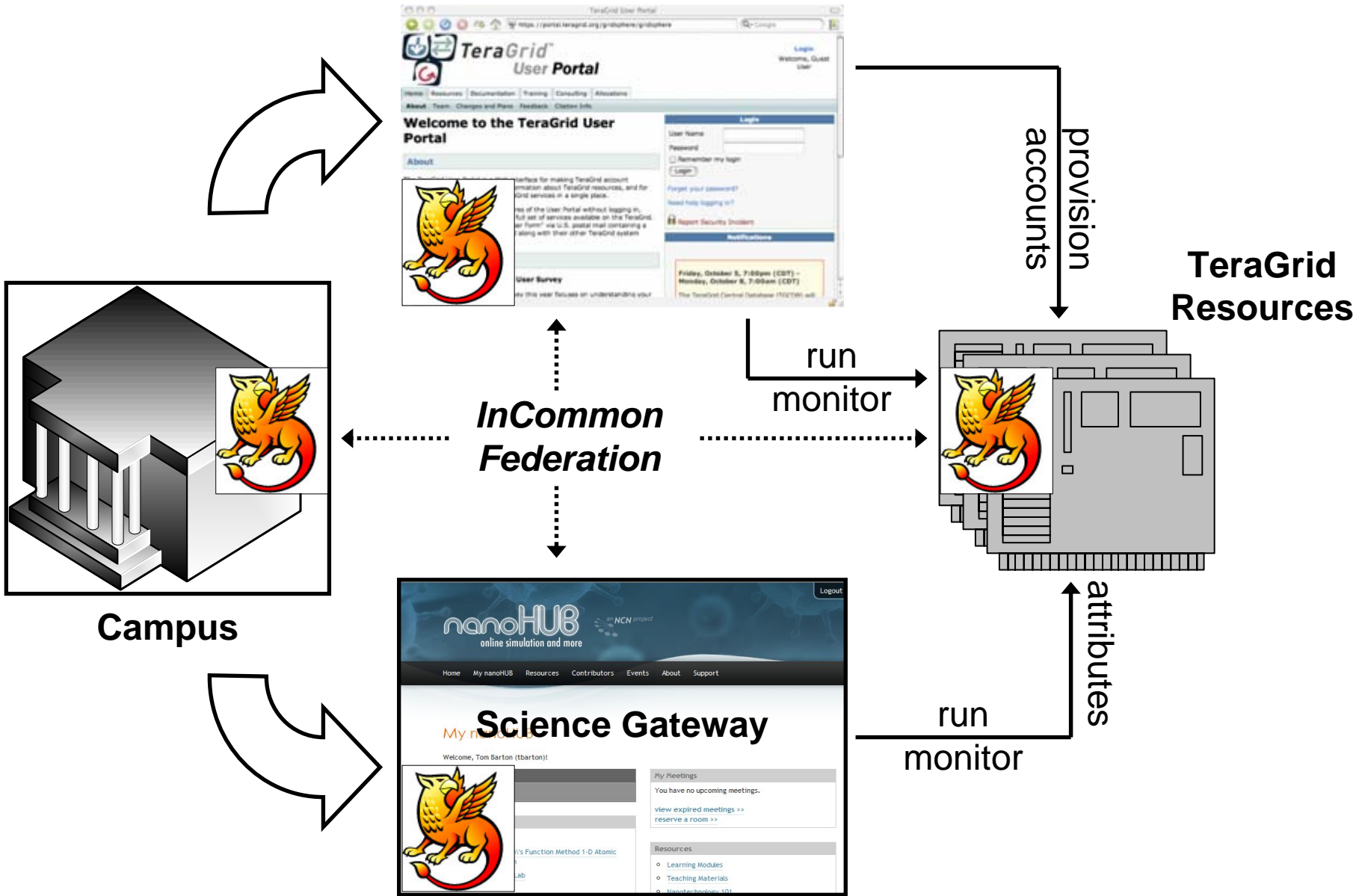
- Document high-level policy & procedure
 - What attributes are needed & why?
 - How are they handled?
- Agree to coordinate as necessary with other participants
- Status of privacy & security policies

Campus Joining InCommon

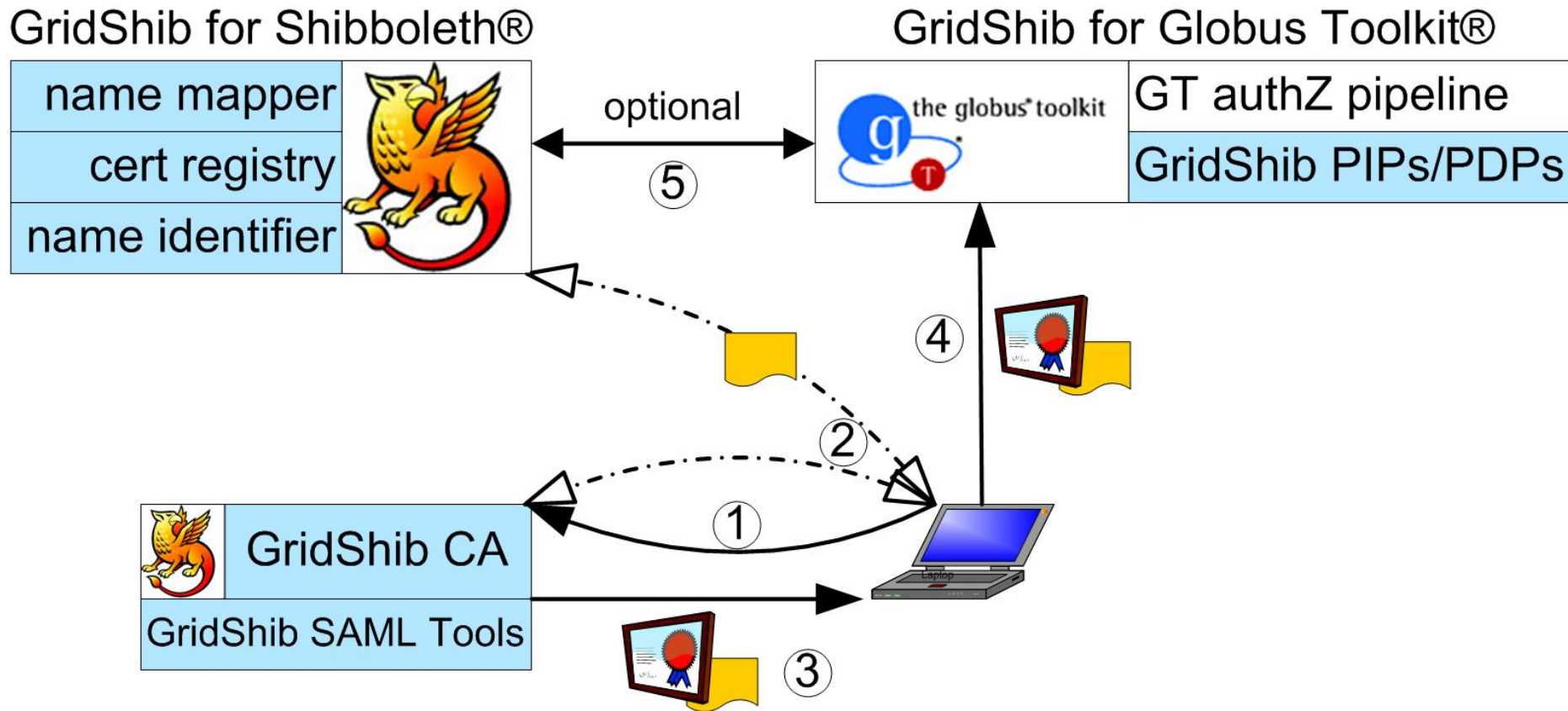
- Document high-level policy & procedure
 - Who do you credential?
 - A little about your IdM operation & authentication service(s)
 - What attributes will you provide (conditionally, perhaps)?
- Operate a (shibboleth) IdP

TeraGrid Federated Identity Testbed

- Prove that Shibboleth and GridShib technology can work with TeraGrid
- Demonstrate that campus identity management & security practices are sufficient
- Determine needed enhancements to internal TeraGrid processes
 - Account provisioning
 - Access management
 - Auditing
 - User support systems and processes



GridShib Components



GridShib for GT

- v0.5.2 PIPs & PDP
 - SAMLAuthnAssertionPIP
 - Extract NameIdentifier from SAML authN assertion embedded in EEC or PC
 - ShibbolethPIP
 - Query SAML AA
 - SAMLMapPIP
 - Map attributes in user's security context (VOMS or SAML) to accounts
 - ShibbolethPDP
 - consults GridMap, VomsPIP, ShibbolethPIP, and SAMLMapPIP (in that order)
- v0.6 PIPs
 - SAMLAssertionPushPIP
 - AttributeAcceptancePIP

GridShib SAML Tools

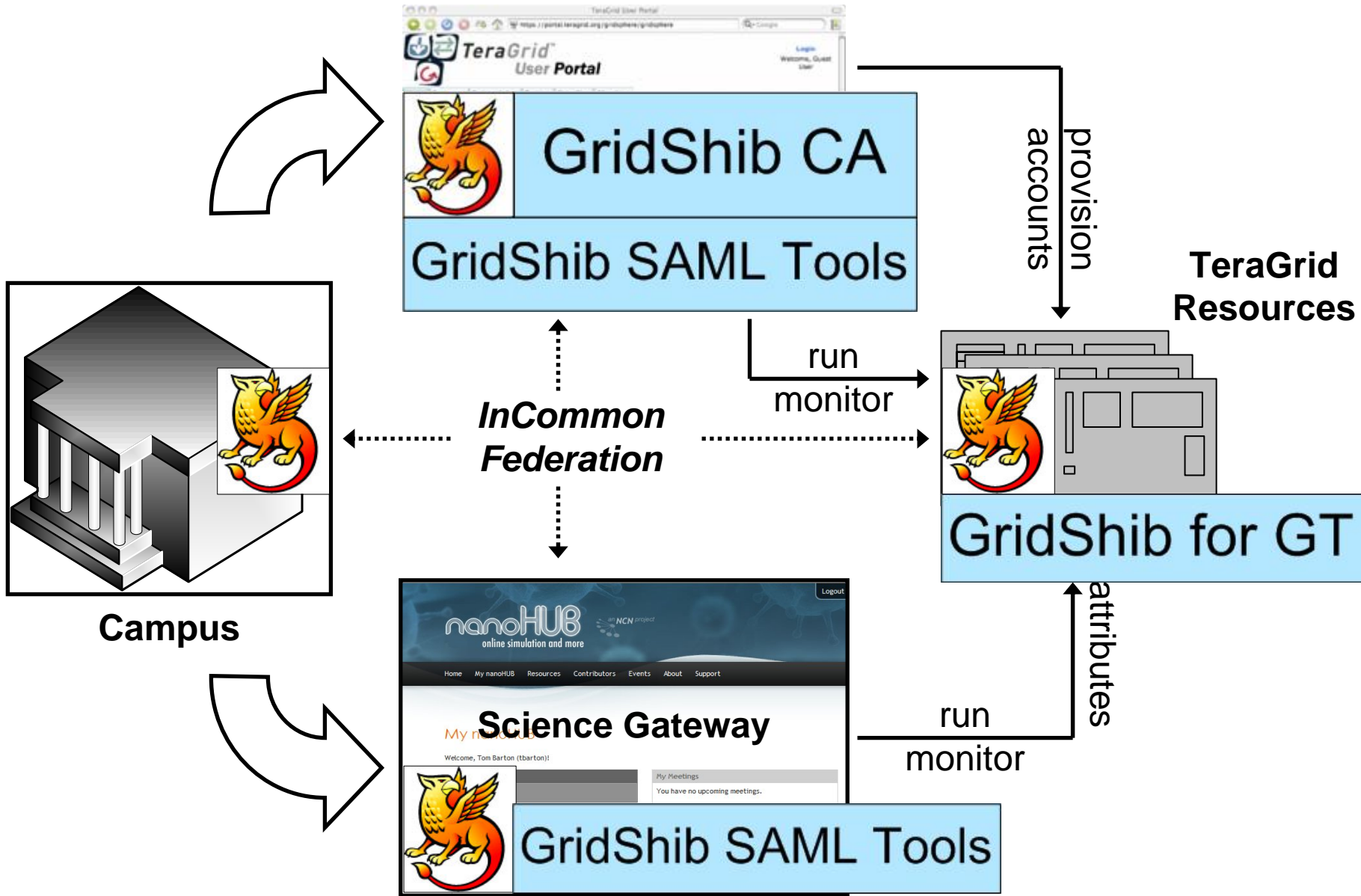
- 4 tools
 - Globus Toolkit SAML Issuer Tool
 - Shibboleth SAML Issuer Tool
 - SAML Attribute Query Client
 - SAML X.509 Binding Tool
- Issue or request SAML assertions and optionally bind these assertions to X.509 proxy certificates
 - Eg: incorporate VO attributes into proxy cert

GridShib CA

- Shibbolized online CA that produces RFC 3820 proxy certs with DN configurable from shibboleth attributes
 - Optionally contain SAML attribute statements within the cert
- Integrated GridShib SAML Tools
- Standalone CA or integrated with MyProxy CA
- Uses Java Web Start to deliver certs to user's PC

GridShib for Shibboleth

- For “legacy” use case
- Cert registry
 - Associate previously-issued EECs with campus identity
- Name identifier Shibboleth plug-in
 - support DN-style name identifiers
- Name mapper Shibboleth plug-in
 - resolve DNs into campus identity using cert registry



DEMO?