GridShib
Grid/Shibboleth
Interoperability

http://gridshib.globus.org

MWSG

March 1, 2007

Tom Barton[1], Tim Freeman[1], Kate Keahey[1], Raj Kettimuthu[1], Tom Scavo[2], Frank Siebenlist[1], Von Welch[2]

[1]University of Chicago

[2]NCSA/University of Illinois

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Acknowledgments

- **GridShib is a project funded by the NSF Middleware Initiative**
  - Collaboration between NCSA and U. Chicago/ANL
  - NMI awards 0438424 and 0438385
  - Opinions and recommendations are those of the authors and do not necessarily reflect the views of the National Science Foundation.
- **Globus Incubator/Open Source**
  - http://dev.globus.org/wiki/Incubator/GridShib
- **Also many thanks to Internet2**

GridShib Goals

- **Allow the Grid to scale by leveraging existing campus identity management (IdM)**
  - Consider Shibboleth as the interface to campus IdM systems
  - Get out of identity management game
- **Making joining the Grid as easy as possible for users**
  - No separate long-term credential for Grid access to manage
  - No new passwords, certificates, etc
- **Allow campuses attributes and VO attributes to be aggregated and used by the Grid for authorization**
  - Allow for scalability in user base through attribute-based authorization - I.e. know groups of users instead of individual users

Why Shibboleth?

- What does Shibboleth bring to the table?
- A large (and growing) installed base on campuses around the world
- Professional development and support team
- A standards-based, open source implementation
- A standard attribute vocabulary (eduPerson)

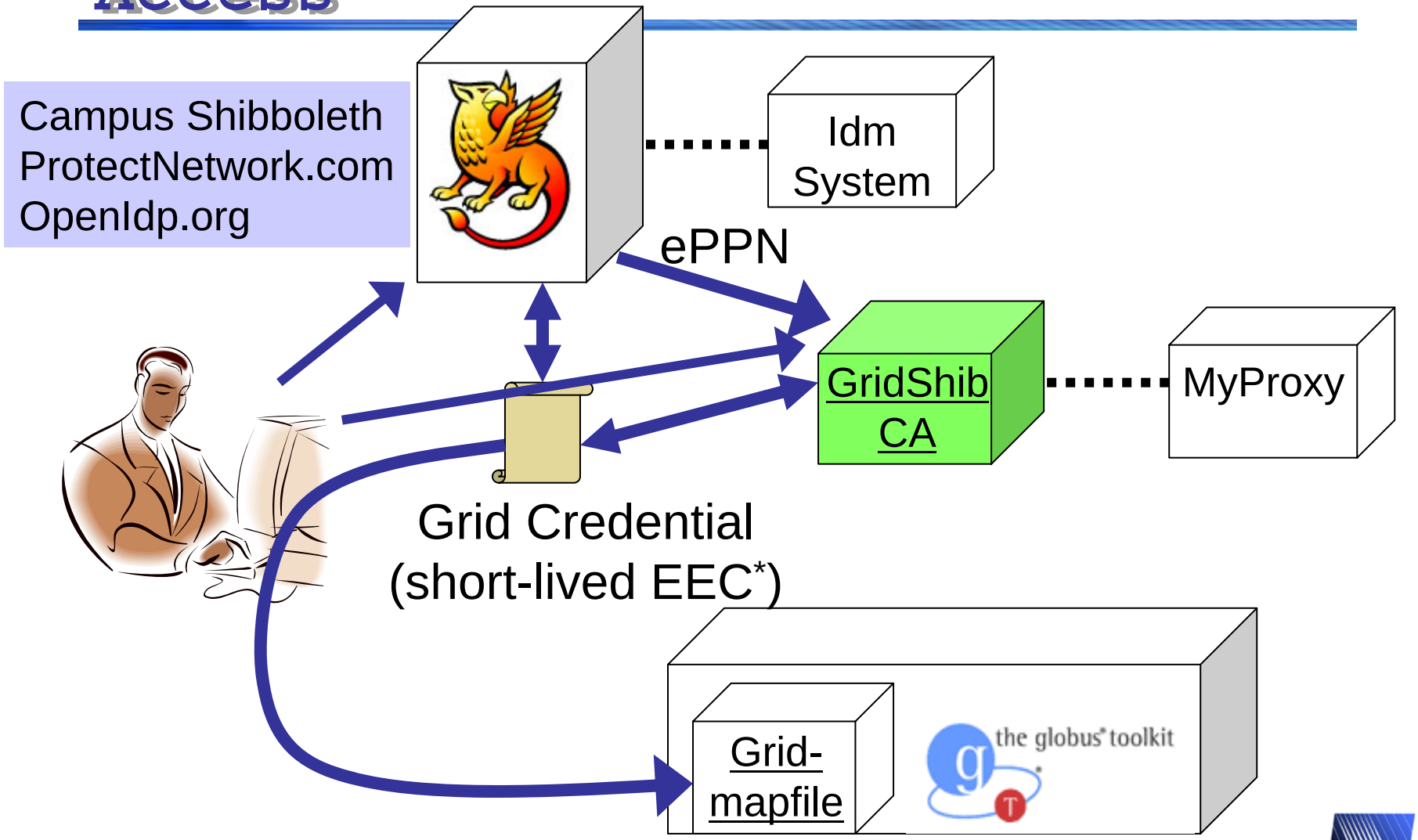
GridShib Software Components

- ***GridShib for Globus Toolkit***
  - A plugin for GT 4.0
- ***GridShib for Shibboleth***
  - A plugin for Shibboleth 1.3 IdP
- ***GridShib CA***
  - A web-based CA for new grid users
- ***GridShib SAML Tools***
  - Tools for portals and users to embed attributes into X.509 credentials
- **All at: http://gridshib.globus.org/**

Deployment Scenarios

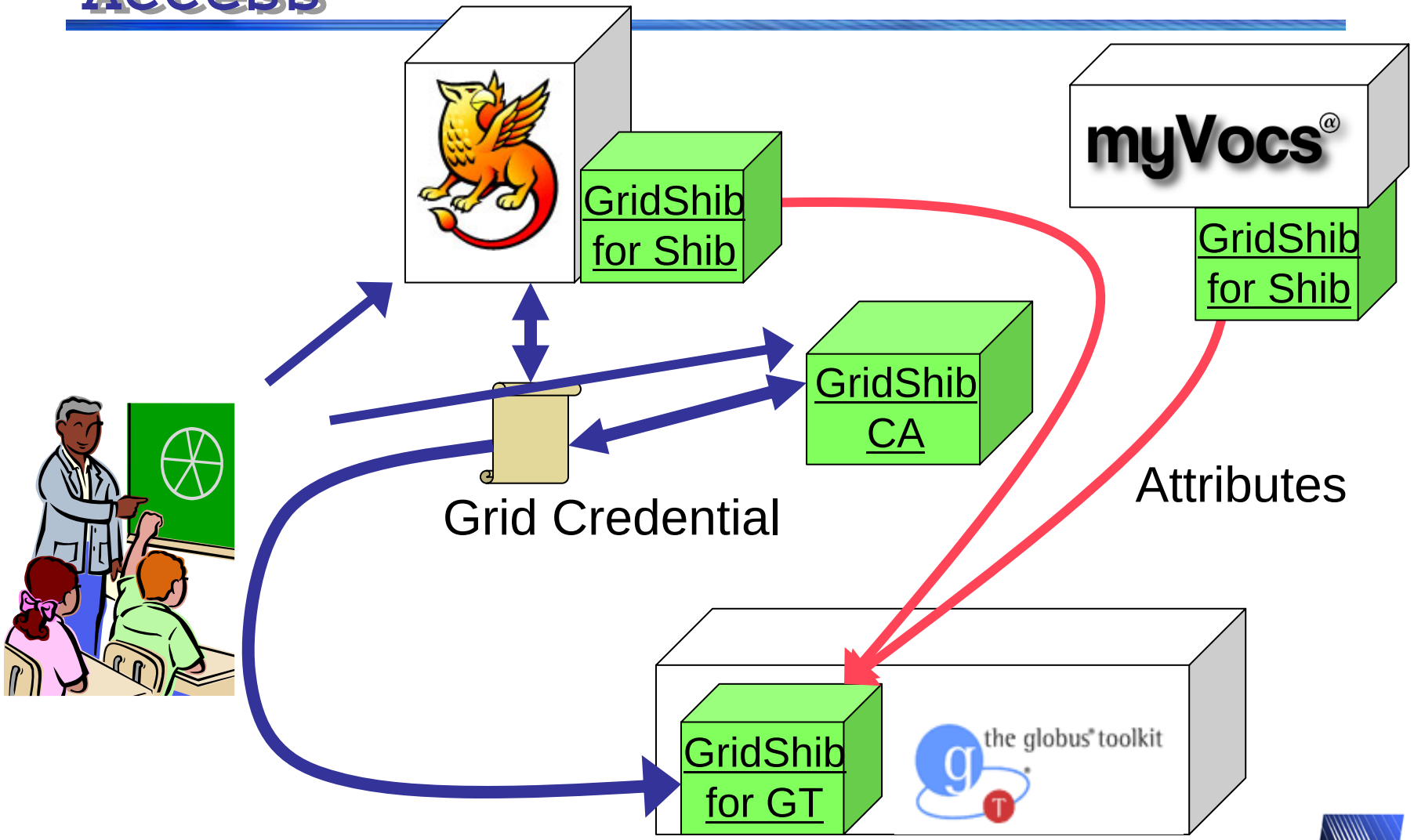
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Shibboleth-authenticated Grid Access

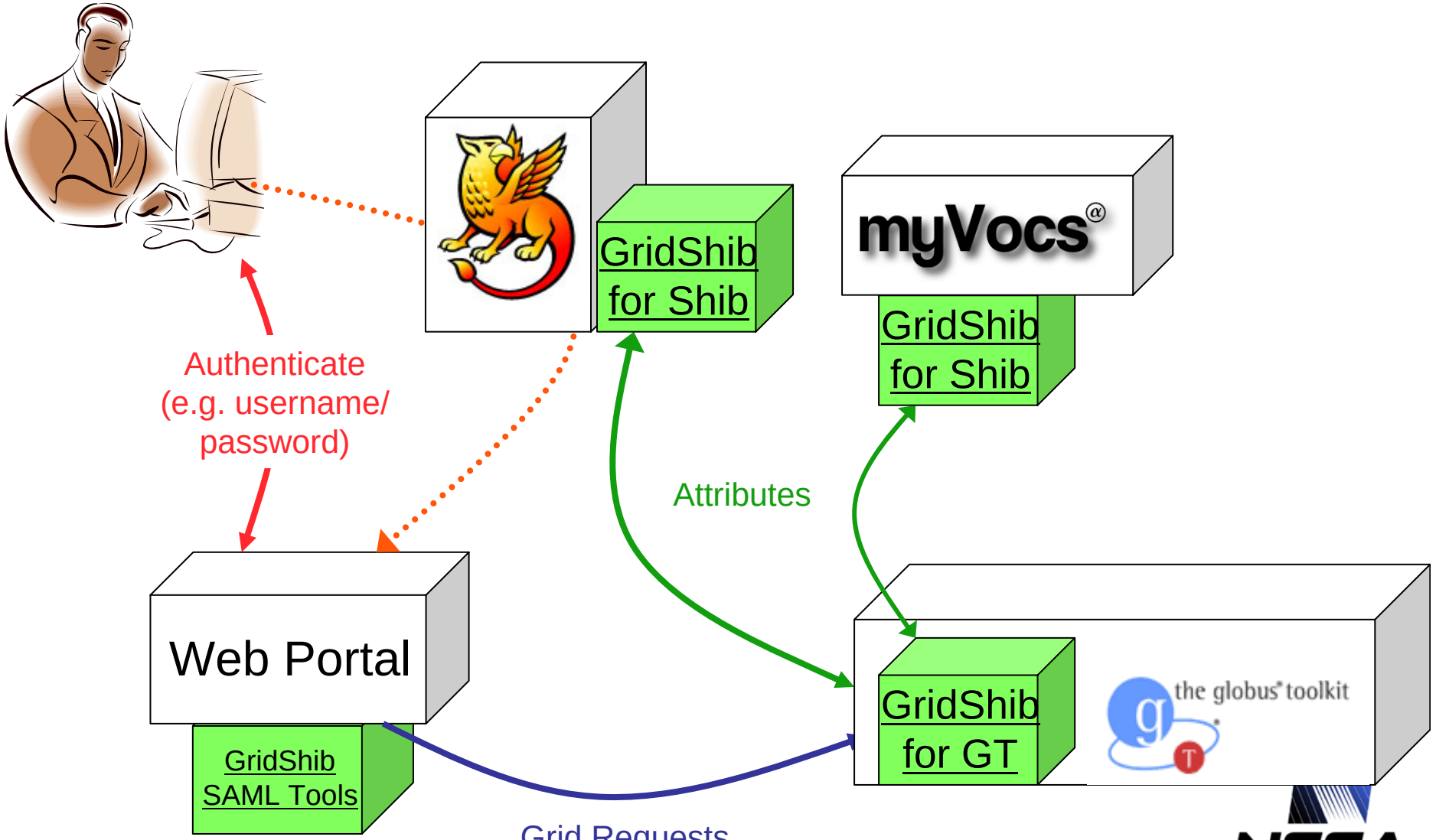


*O(8 hours), <1M secs

Shibboleth-authorized Grid Access



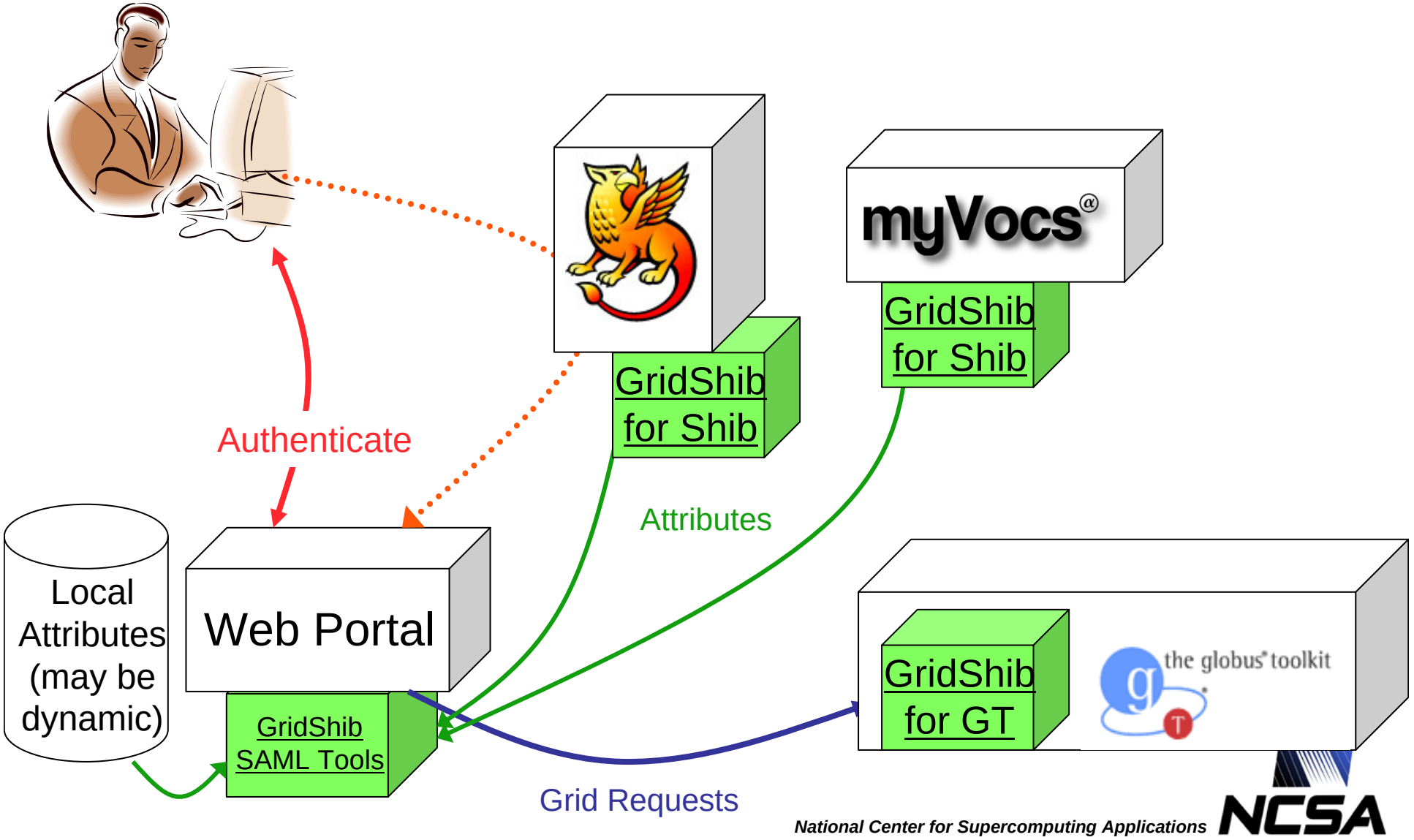
Community Access via Science Gateway



Attribute Push

- **Turning to attribute push**
- **Our observation is that most Grid use cases want:**
  - Persistent Id from Home Institution
  - Attributes from VO
- **Shib/X.509 Gateway is natural point to collection Attributes from home institution and combine with VO attributes and push to Grid**
  - Gateway could be the GridShib-CA or a domain-portal, e.g. a TeraGrid Science Gateway
  - Attributes may be static or dynamic

Attribute Push Scenario



Our Roadmap

- **We will now present current plans and timelines**
- **Roadmap online at GridShib dev.globus incubator site**

  http://dev.globus.org/wiki/GridShib_Development_Roadmap
- **Roadmap will be maintained as work progresses, check web page for updates**

GridShib for Globus Toolkit

- ***GridShib for Globus Toolkit* is a plugin for GT4**
- **Features:**
  - SAML Authentication consumer
  - SAML attribute consumption
  - Attribute-based access control
  - Attribute-based local account mapping
  - SAML metadata consumption

GridShib for GT 0.5.1

- **Announced Feb 15**
- **Compatible with both GT4.0 and GT4.1**
  - GT4.1 introduces powerful authz framework
  - Separate binaries for each GT version
  - Source build auto-senses target GT platform
- **Combined VOMS/SAML attribute to account mapping**
  - Checks in this order and continues to fall back if no match/authz is granted: gridmap, VOMS, Shibboleth/SAML

GridShib for GT 0.6

- **Expected March 2007**
- **Full-featured attribute push PIP**
  - Compatible with current GridShib Attribute Tools
- **More powerful attribute-based authz policies**
  - Allow unique issuer in authz policy rules

GridShib SAML Tools

- **Tools for creating SAML and binding to Grid Credentials**
- **Used to direct GridShib for GT to appropriate Shibboleth AA**
  - Addressing WAYF
- **Directs GridShib for GT as what what identifier to use in SAML attribute request**
  - Can alleviate need for Shibboleth Idp changes
- **Allows binding of Attributes from Shibboleth or generated locally**
  - To be consumed by GridShib for GT 0.6.0
- **Current version 0.1.2**

GridShib SAML Tools 0.2.0

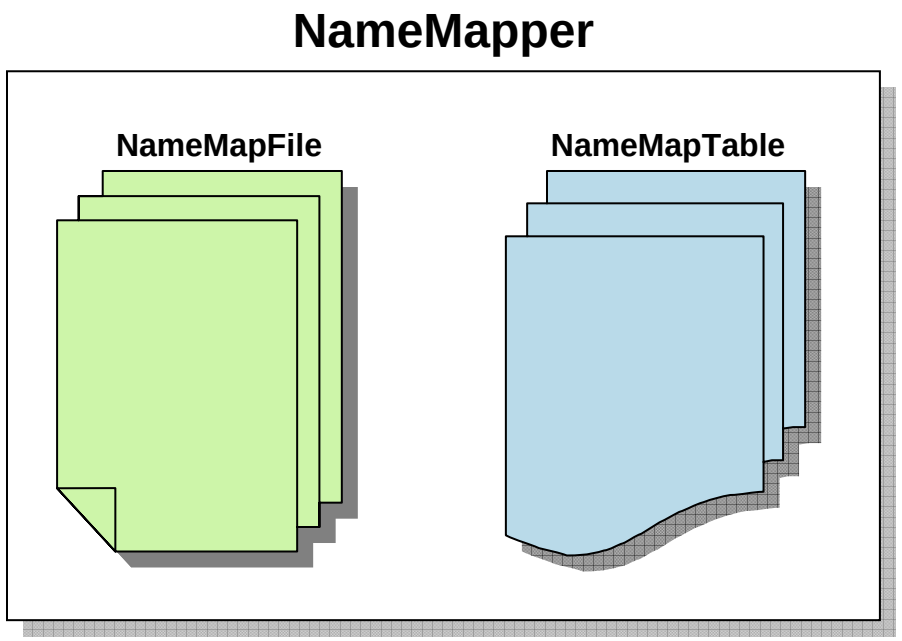
- Target release date: February 2007
- Same command-line interface as v0.1.x (but with more options)
- Leverages Shibboleth Attribute Resolver to support more complicated attribute requirements
- Support for nested SSO Response
- Enhanced logging
- Java API for Portal developers

GridShib for Shibboleth

- ***GridShib for Shibboleth* is a plugin for a Shibboleth IdP v1.3 (or later)**
- **Features:**
  - Name Mapper
  - SAML name identifier implementations
    - X509SubjectName, emailAddress, etc.
  - Certificate Registry

GridShib Name Mapper

- **Users may be known by a number of names**
- **The Name Mapper is a container for name mappings**
- **Multiple name mappings are supported:**
  - File-based name mappings
  - DB-based name mappings



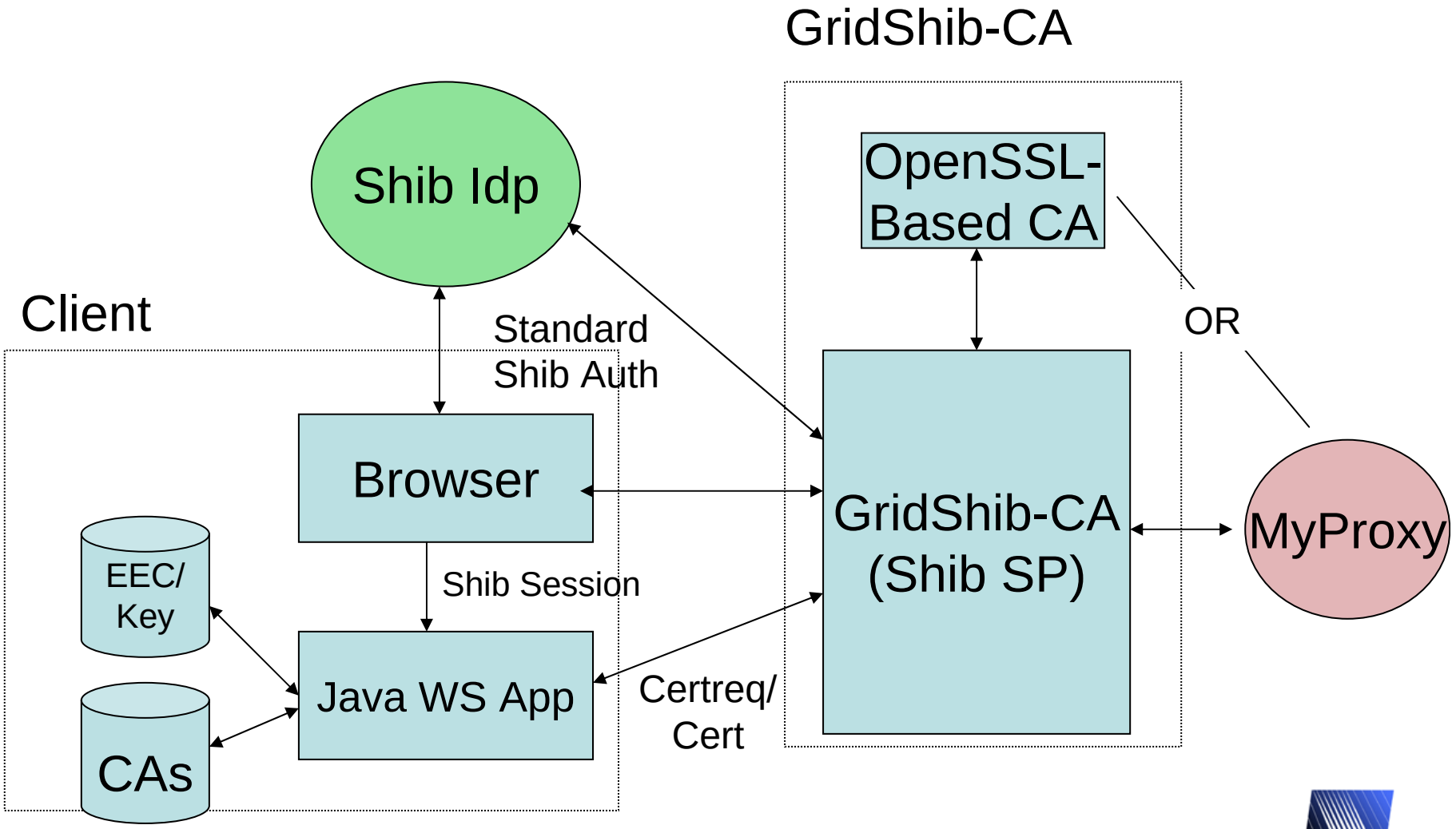
GridShib Certificate Registry

- **A *Certificate Registry* is integrated into GridShib for Shibboleth**
- **An established grid user authenticates and registers an X.509 end-entity cert**
- **The Registry binds the cert to the principal name and persists the binding in a database**
- **On the backend, GridShib maps the DN in a query to a principal name in the DB**

GridShib CA

- **The *GridShib Certificate Authority* is a web-based CA for new grid users**
- **The GridShib CA is protected by a Shib SP and back-ended by the MyProxy Online CA**
  - Or a local OpenSSL-based CA
- **The CA issues short-term credentials suitable for authentication to a Grid SP**
  - Short-lived EEC, similar to MyProxy-CA or KCA
- **Credentials are downloaded to the desktop via Java Web Start**
  - Lots of tricky security details here
- **Version up at https://computer.ncsa.uiuc.edu/**
  - Can be used by anyone in InQueue or with OpenIdp or ProtectNetwork login

GridShib-CA Architecture



More detail: http://gridshib.globus.org/docs/gridshib-ca-0.3.0/process-flow.html

GridShib CA 0.3

- **Substantial improvement over version 0.2**
- **More robust protocol**
- **Installation of trusted CAs at the client**
- **Pluggable back-end CAs**
  - Uses an openssl-based CA by default
  - A module to use a MyProxy CA is included
- **Certificate registry functionality**
  - A module that auto-registers DNs with myVocs

GridShib CA 0.4

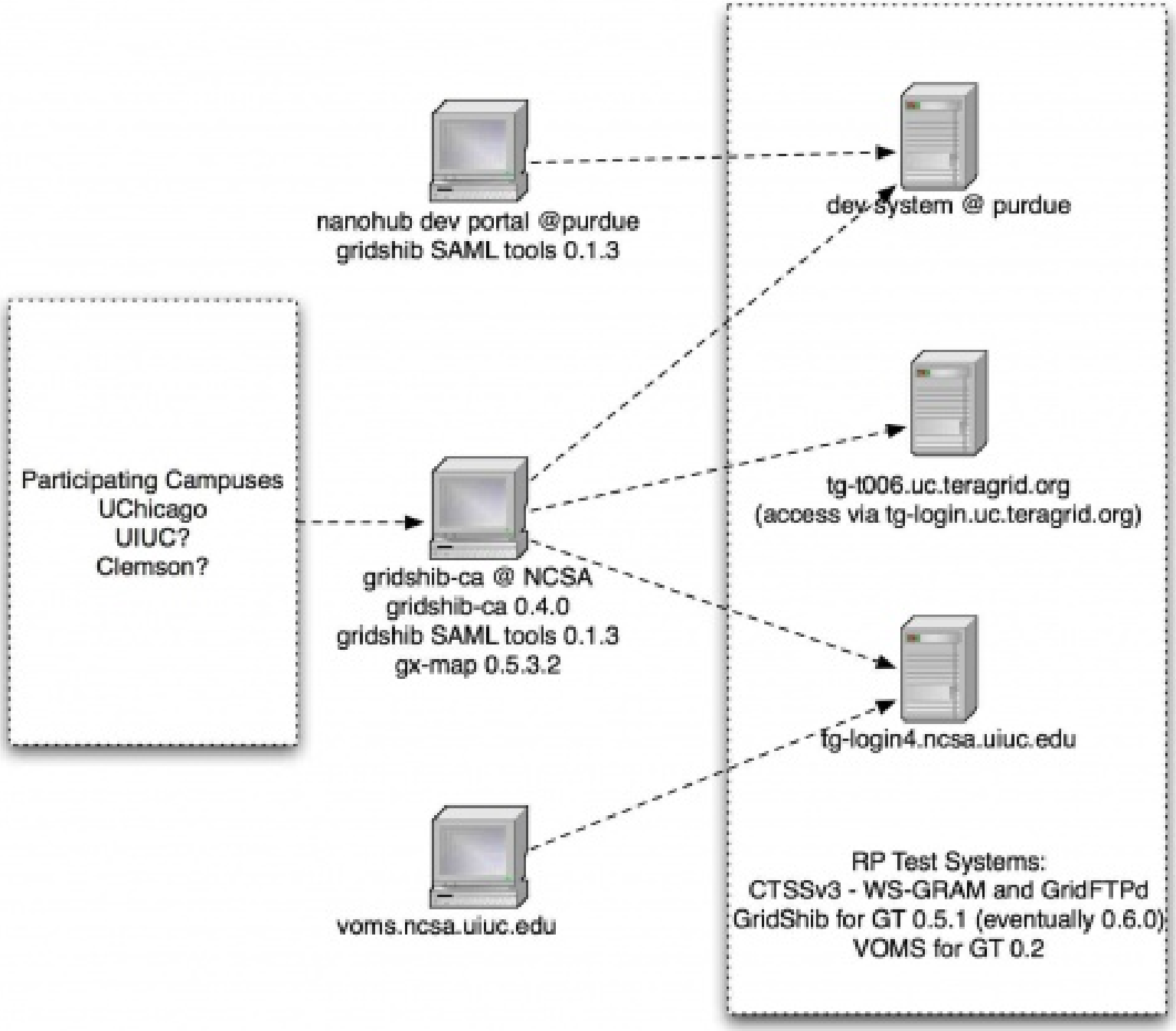
- **Target release: March 2007**
- **Incorporate improvements from initial deployments and requirements from TeraGrid**
  - Fall back to default SSLSocketFactory on error (Bug 4875)
  - Create CA with domain name components (Bug 4887)
  - Integrate GridShib SAML Tools to bind simple attribute assertion to EEC
  - Bind IdP entityID to SIA extension
  - Handle creating DN from mix of attributes (Bug 4889)

TeraGrid testbed

- **Testbed for Federated Identity Management and Attribute-based Authorization**
  - Building on Shibboleth, GridShib
- **Goals:**
  - Allow for scalable access by leveraging campus authentication - remove Idm burden from TeraGrd
  - Allow for attribute-based authorization to define communities
  - Ease of use for users - no management of long-term Grid credentials
  - Interoperability with OSG, others.
- **If this sounds like something you would be interested in participating in please talk to me**

TG: Plans/Progress

- **Rollout attribute-based authz to handful of RP nodes**
  - Test systems or alternative head nodes for HPC systems
  - Integrating with CTSSv3
  - CTSSv4 will be vdt-based, investigate interactions with GUMS/PRIMA
- **Prototype portal - nanoHub prototype @ Purdue**
- **Establish GridShib-CA for TG**
- **Policies, procedures**


nanohub dev portal @purdue
gridshib SAML tools 0.1.3
dev system @ purdue
Participating Campuses
UChicago
UIUC?
Clemson?
gridshib-ca @ NCSA
gridshib-ca 0.4.0
gridshib SAML tools 0.1.3
gx-map 0.5.3.2
tg-t006.uc.teragrid.org
(access via tg-login.uc.teragrid.org)
fg-login4.ncsa.uiuc.edu
voms.ncsa.uiuc.edu
RP Test Systems:
CTSSv3 - WS-GRAM and GridFTPd
GridShib for GT 0.5.1 (eventually 0.6.0)
VOMS for GT 0.2

TG Testbed: Issues

- **What do Grids need from campuses?**
  - Persistent Identifier - targetedId vs ePPN
  - Legal name (displayName)
- **Incident response**
  - Grid sites must have ability to de-authorize user quickly
  - What's the next step?
  - Campus must agree to "help"
  - Campuses want to be informed of issues
  - Need POC (7/24 probably not always available)
  - Define responsibility split

Issues cont

- **What attribute information do we log and how?**
  - Obviously record information related to authorization
  - Keep other attributes? Any privacy concerns?
  - SAML/Shibboleth attributes get long fast
    - attribute name = urn:mace:dir:attribute-def:role
    - attribute namespace = urn:mace:shibboleth:1.0:attributeNamespace:uri
    - attribute value = owner@teragrid-test-one
  - Syslog line limits get hit quickly with naïve schemes

Questions…