


Attribute-based Authorization for Science Gateways Using GridShib

Tom Scavo

trscavo@ncsa.uiuc.edu

National Center for Supercomputing Applications

University of Illinois at Urbana-Champaign

May 14, 2008


Overview

- GridShib Project Update
  - GridShib SAML Tools
  - GridShib for Globus Toolkit
- The TeraGrid Science Gateway Use Case
  - Community Account Model
  - Grid Authorization Model for Science Gateways
  - TeraGrid Deployment Strategy
  - Federated Identity Model for Science Gateways

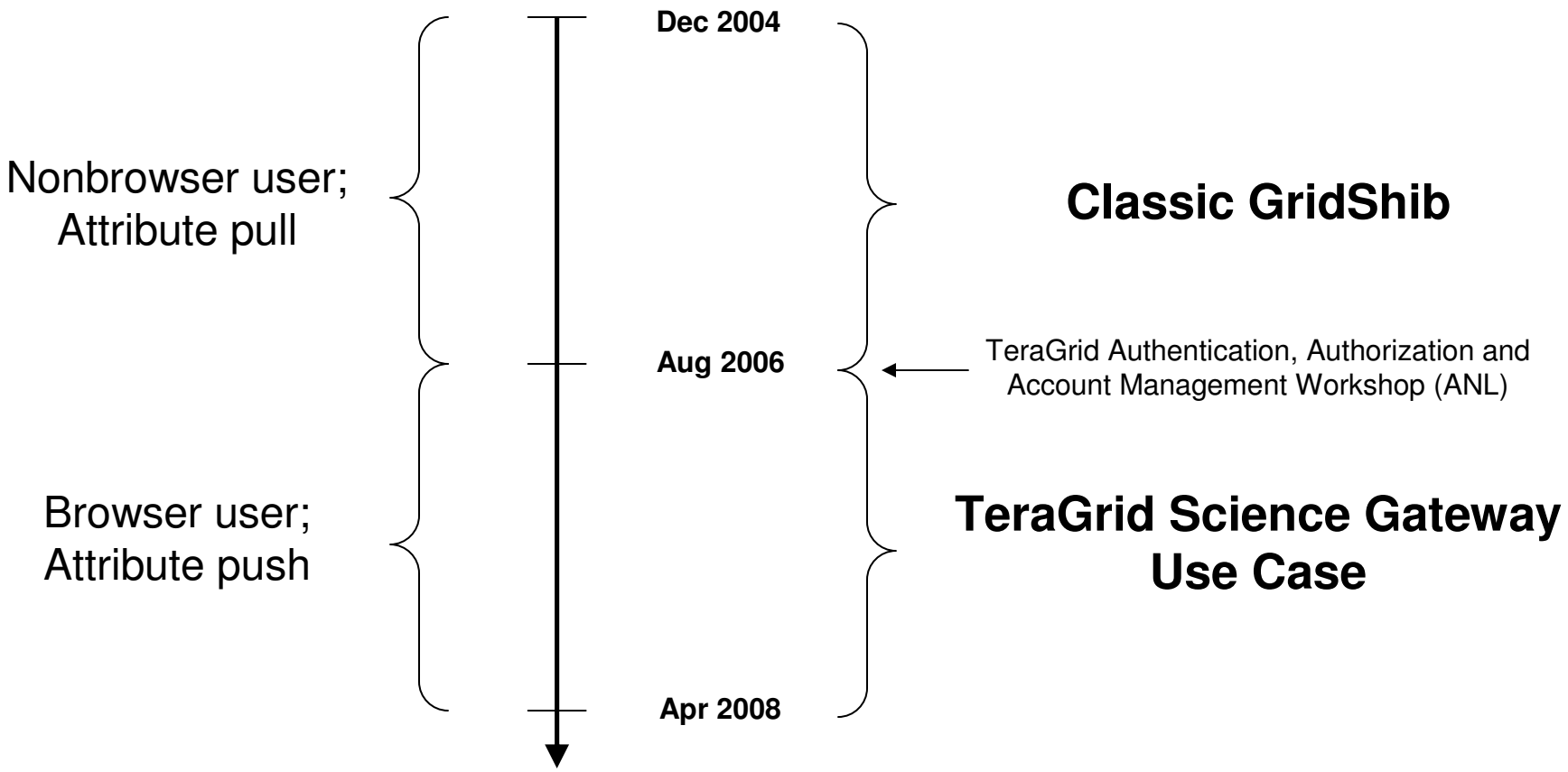

Acknowledgments

- Original Project PIs
  - Von Welch, Tom Barton, Kate Keahey, Frank Siebenlist
- Developers
  - Rachana Ananthakrishnan, Jim Basney, Tim Freeman, Raj Kettimuthu, Terry Fleury, Tom Scavo

- The GridShib work was funded by the NSF National Middleware Initiative (NMI awards 0438424 and 0438385). Opinions and recommendations in this paper are those of the authors and do not necessarily reflect the views of NSF.
- The Science Gateway integration work is funded by the NSF TeraGrid Grid Integration Group through a sub-award to NCSA.


GridShib Project Update

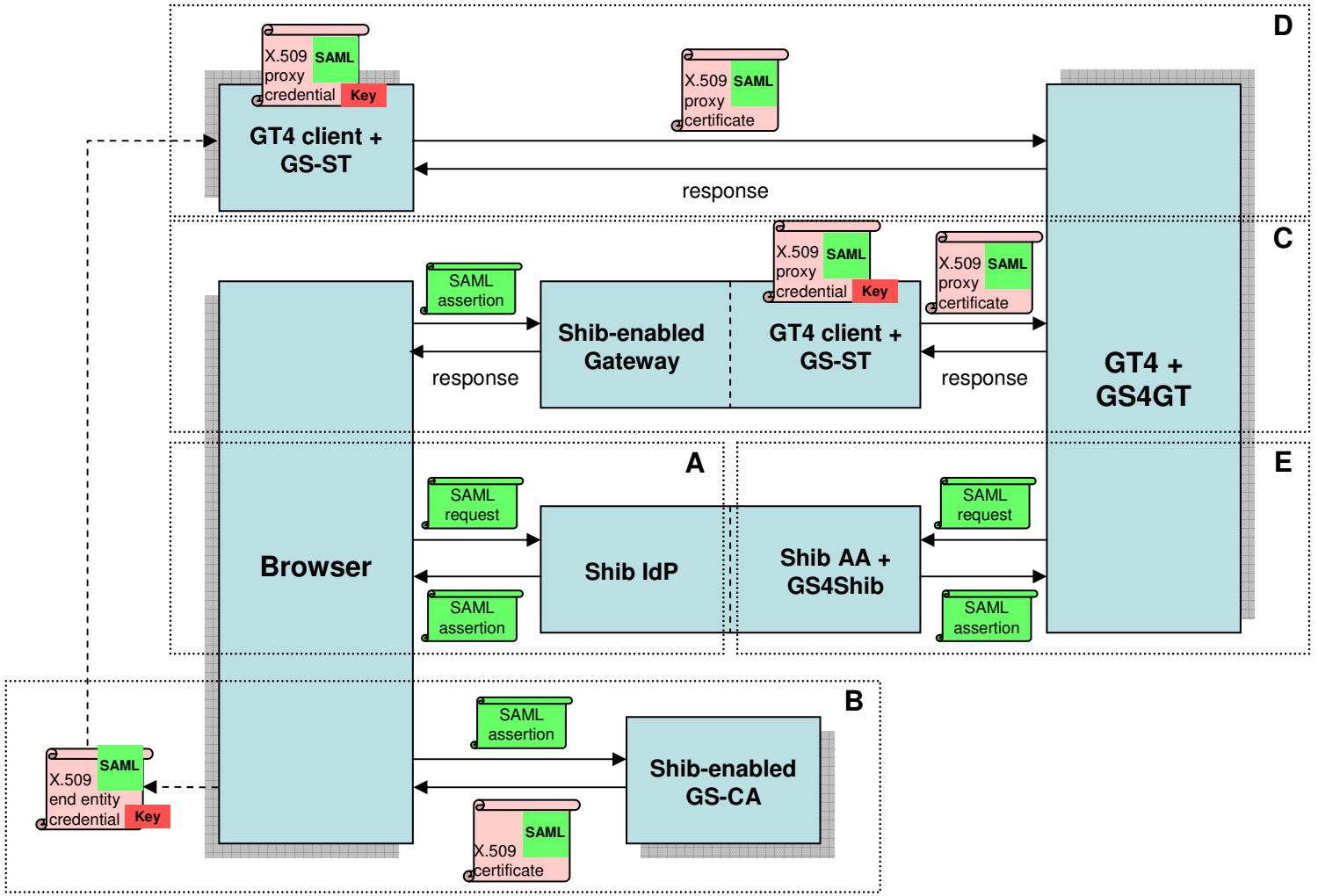
History of GridShib



GridShib Software

- *GridShib for GT*
  - Consumes X.509-bound SAML assertions issued by the GridShib CA or the GridShib SAML Tools. Issues SAML attribute queries to a Shibboleth IdP with GridShib for Shibboleth installed.
- *GridShib for Shibboleth*
  - Responds to attribute queries from GridShib for GT.
- *GridShib CA*
  - Issues short-lived X.509 credentials to browser users.
- *GridShib SAML Tools*
  - Issue or requests SAML assertions and optionally binds these assertions to X.509 proxy certificates.

Deployment Scenarios



http://gridshib.globus.org/docs/gridshib/deploy-scenarios.html


Recent Releases

- GridShib for Globus Toolkit v0.6.0
  - Released April 30, 2008
- GridShib SAML Tools v0.3.2
  - Released March 20, 2008
- http://gridshib.globus.org/download.html


GridShib SAML Tools

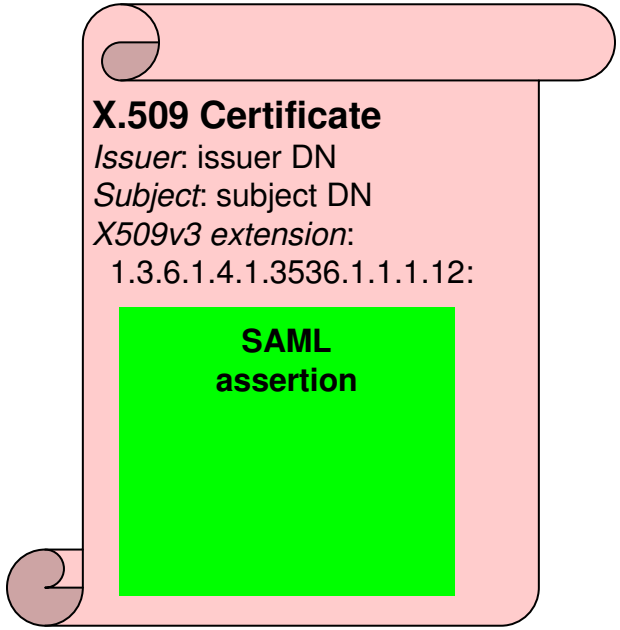
- The *GridShib SAML Tools* (GS-ST) are a standalone suite of Java-based client tools
  - Binds a SAML assertion to an X.509 proxy certificate
  - The same X.509-bound SAML token can be transmitted at the transport level or the message level (using WS-Security X.509 Token Profile)
- Includes the *GridShib Security Framework*, an API for producing and consuming X.509-bound SAML tokens
- GS-ST is a **SAML producer**

GS-ST Features

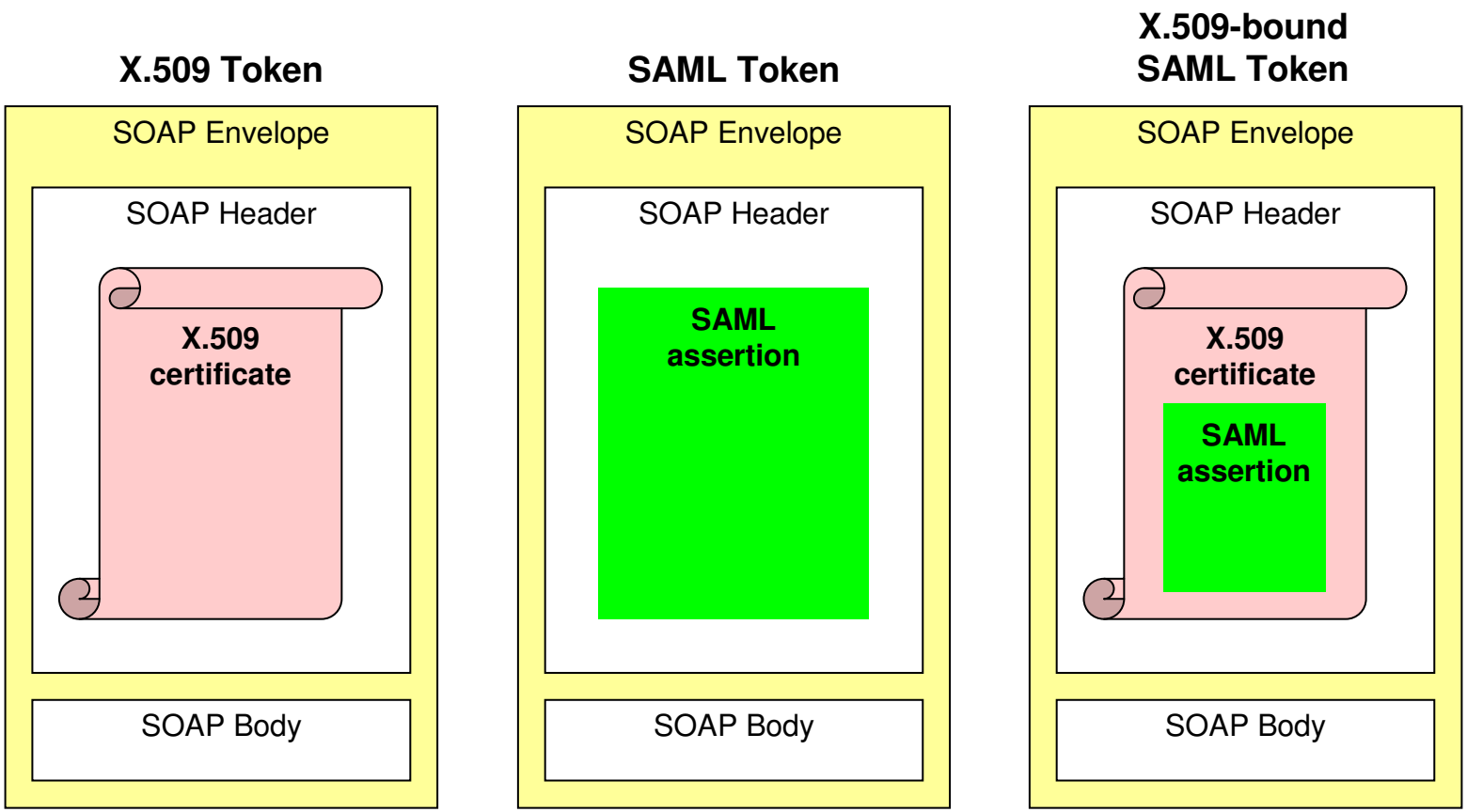
- Easily installed and configured
- Binds arbitrary content (e.g., SAML) to a non-critical certificate extension
- Multiple output options (SAML, X.509 proxy credential, DER-encoded ASN.1)
- CLI with shell scripts (UNIX and Windows)
- Includes a Java API for portal developers
- Leverages the *Globus SAML Library*, an enhanced version of OpenSAML 1.1

X.509-bound SAML Token

- GridShib SAML Tools produces *X.509-bound SAML tokens*, a new type of security token that enables attributed-based authorization in X.509-based Grids
- The SAML token is bound to a noncritical X.509v3 certificate extension



Security Tokens



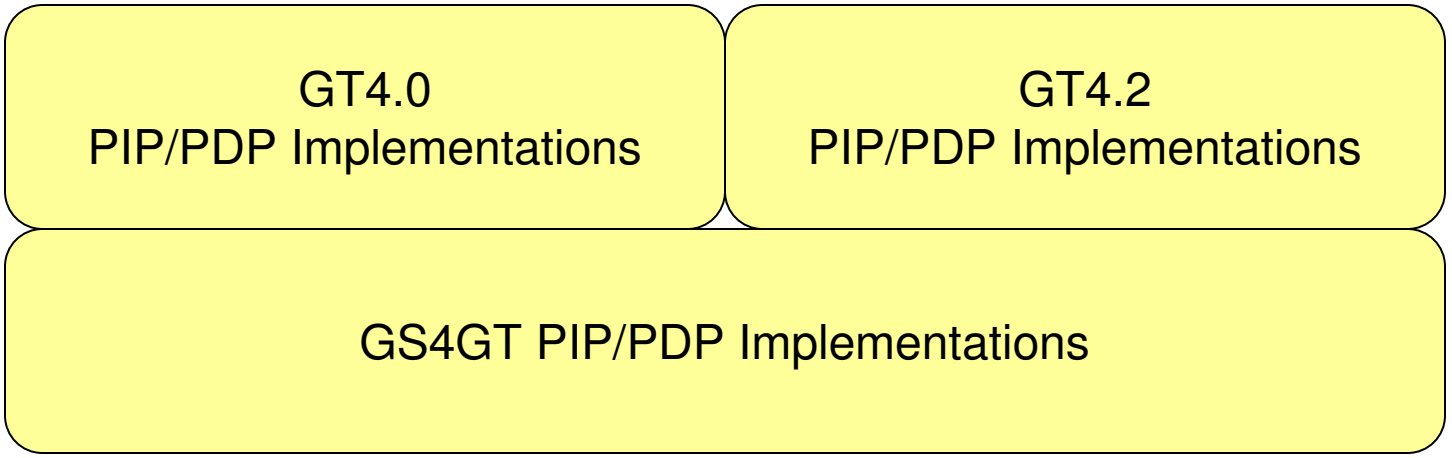
GridShib for GT

- GridShib for GT (GS4GT) is a plug-in for GT 4.x
  - GS4GT is compatible with both GT 4.0 and 4.2
- GS4GT is an implementation of a *Grid Service Provider* (analogous to a Shibboleth Service Provider)
- GS4GT is a **SAML consumer**

GS4GT Features

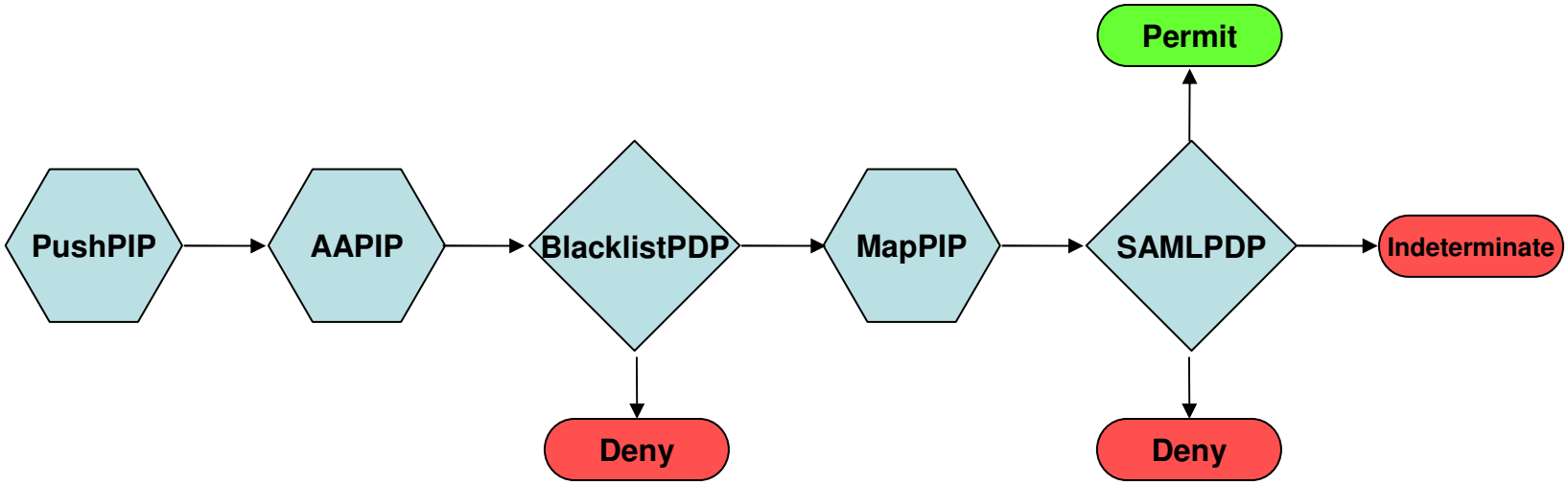
- Introduces *attribute-based authorization* into GT
- Exposes a single comprehensive *policy decision point* called the **`GridShibPDP`**
- Implements an *attribute push* model
- Restricts access based on *blacklists* of IP addresses and/or name identifiers
- Provides *attribute-based account mapping*
- Supports optional *gridmap short-circuiting*
- Defines an *attribute-based authorization policy* language (in XML)

GT4.0/4.2 Compatibility



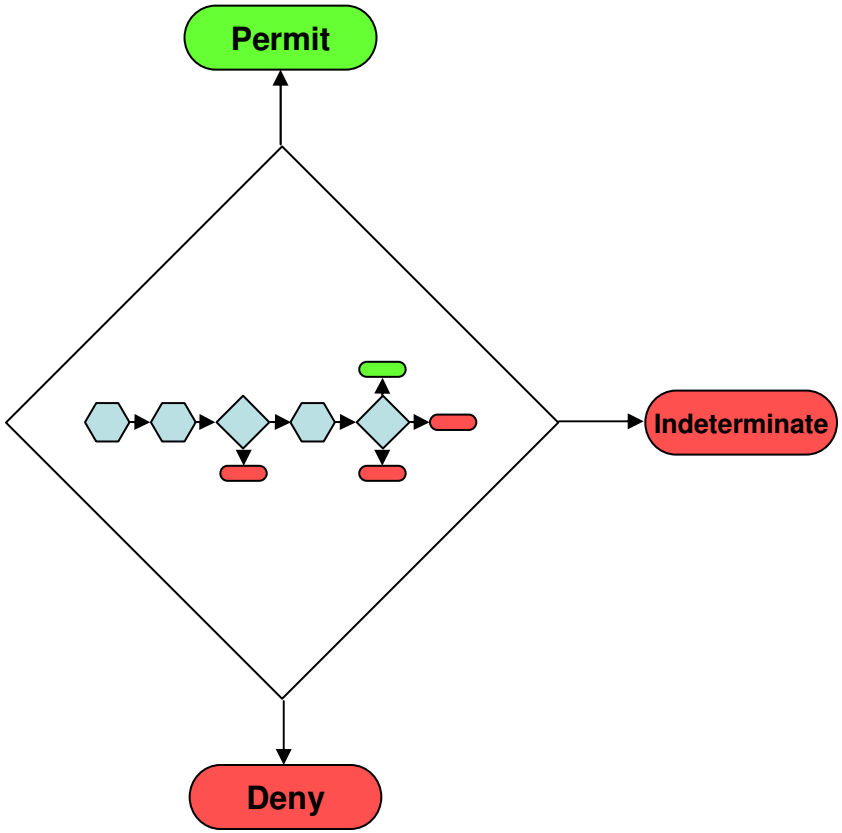
- GS4GT adds a layer of abstraction that permits both GT4.0 and GT4.2 to be supported simultaneously

GridShib Attribute Push

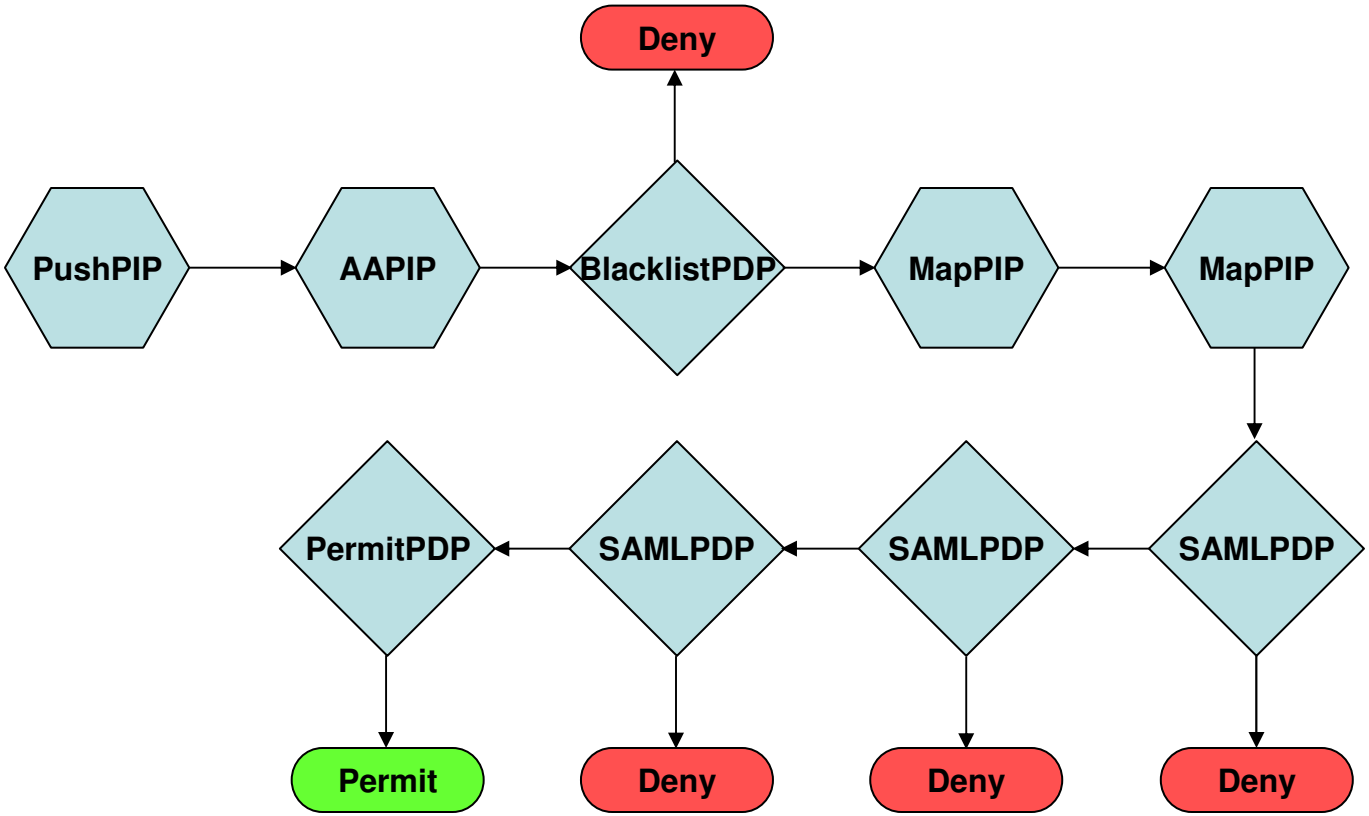


- In GT4.0 (deny-overrides), this works because the PDP is at the end of the chain
- In GT4.2 (permit-overrides), this authz chain does not honor SAMLBlacklistPDP

GridShibPDP



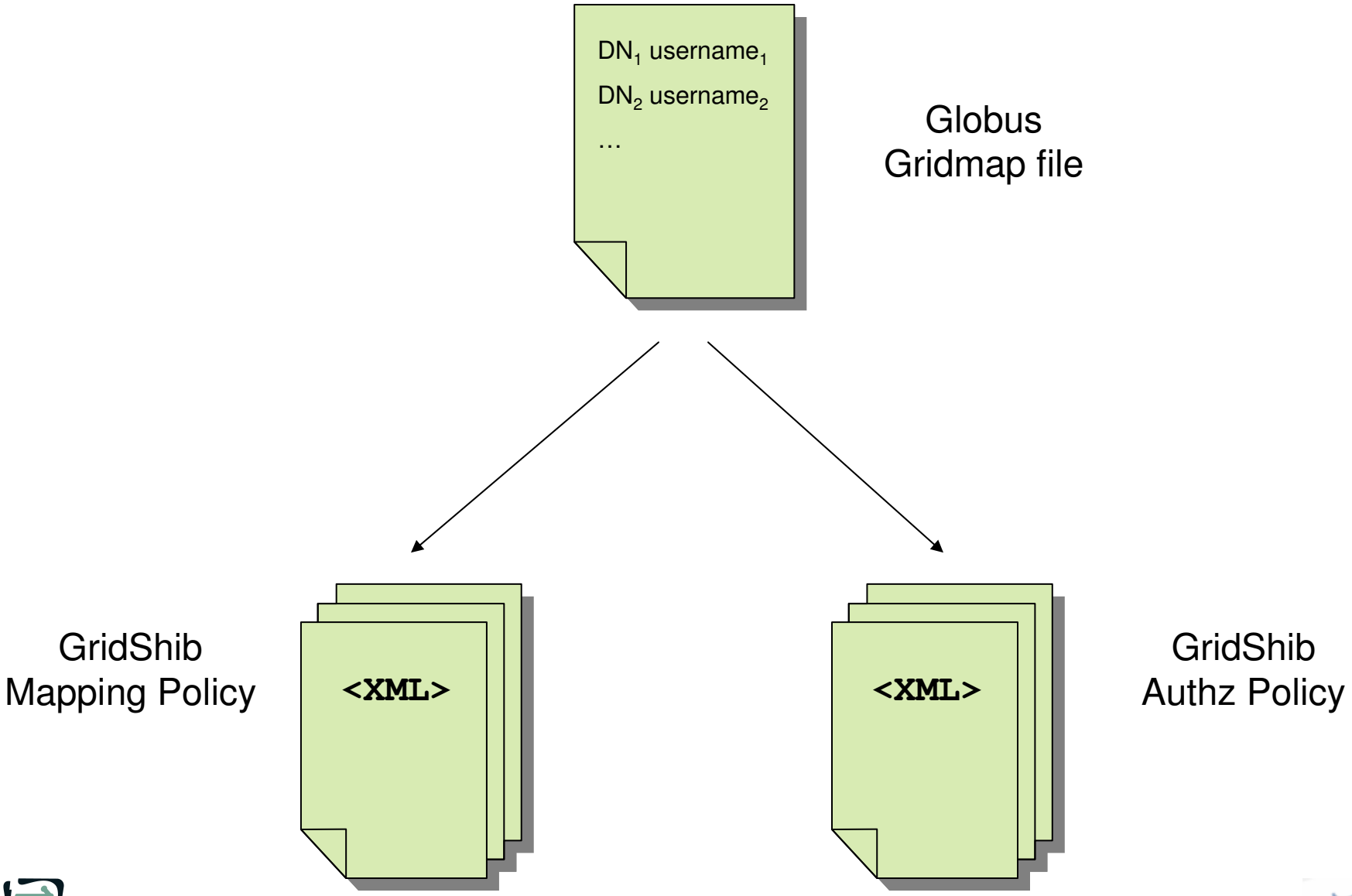
Complex Authz Policy



Gridmap File

- Flat file format:

  DN → [$user_0$, $user_1$, …, $user_{n-1}$]
- Dual function identity-based gridmap file:
  1. Authorization Policy
  2. Username Mapping Policy
- A single gridmap file serves both functions


DN1 username1
DN2 username2
...
Globus
Gridmap file
GridShib
Mapping Policy
<XML>
<XML>
GridShib
Authz Policy

GridShib Policy Files

- Two separate attribute-based policy files:
  1. Authorization Policy

     $[A_0, A_1, \ldots, A_{m\text{-}1}]$

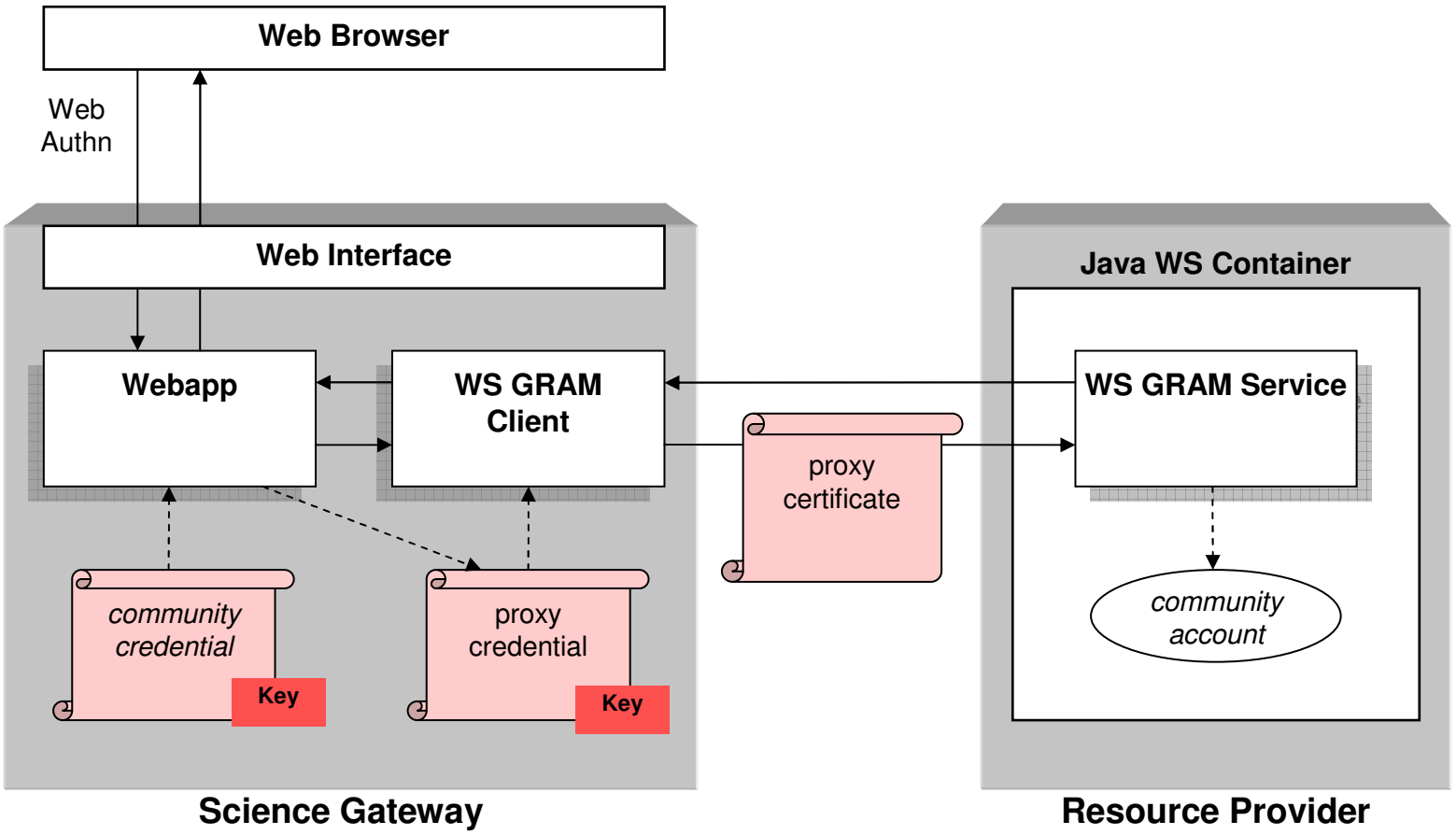
  2. Username Mapping Policy

     $[A_0, A_1, \ldots, A_{m_1\text{-}1}] \rightarrow [user_0, user_1, \ldots, user_{n_1\text{-}1}]$

     $[A_0, A_1, \ldots, A_{m_2\text{-}1}] \rightarrow [user_0, user_1, \ldots, user_{n_2\text{-}1}]$ …
- A single XML-based policy file *may* encapsulate both types of policies

The TeraGrid Science Gateway Use Case

Science Gateway



Community Account Model

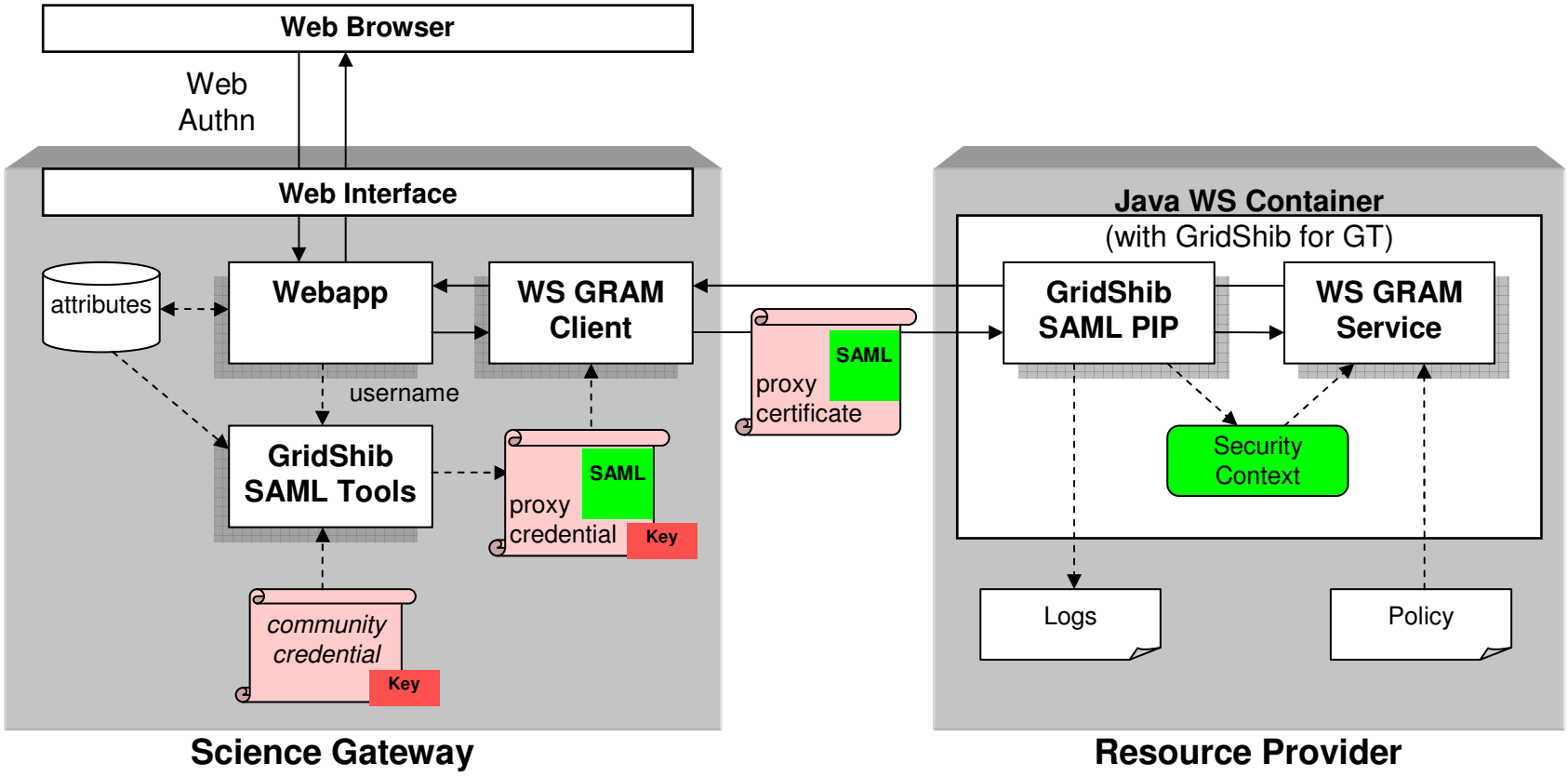
- A *community credential* is issued to each gateway
- The gateway issues proxy certificates (on-the-fly) and makes grid requests on behalf of the user
- This *community account model* is easy to implement but has some significant drawbacks
- **All requests look exactly the same to the resource provider**

Grid Authorization Model

- The proposed model incorporates GridShib SAML Tools at the gateway and GridShib for GT at the resource provider
- Using GridShib SAML Tools, the gateway
  1. issues a SAML assertion containing the user's authentication context and attributes
  2. binds the SAML assertion to a proxy certificate signed by the community credential
  3. authenticates to the resource by presenting the SAML-laden proxy certificate

http://gridfarm007.ucs.indiana.edu/gce07/images/e/e4/Scavo.pdf

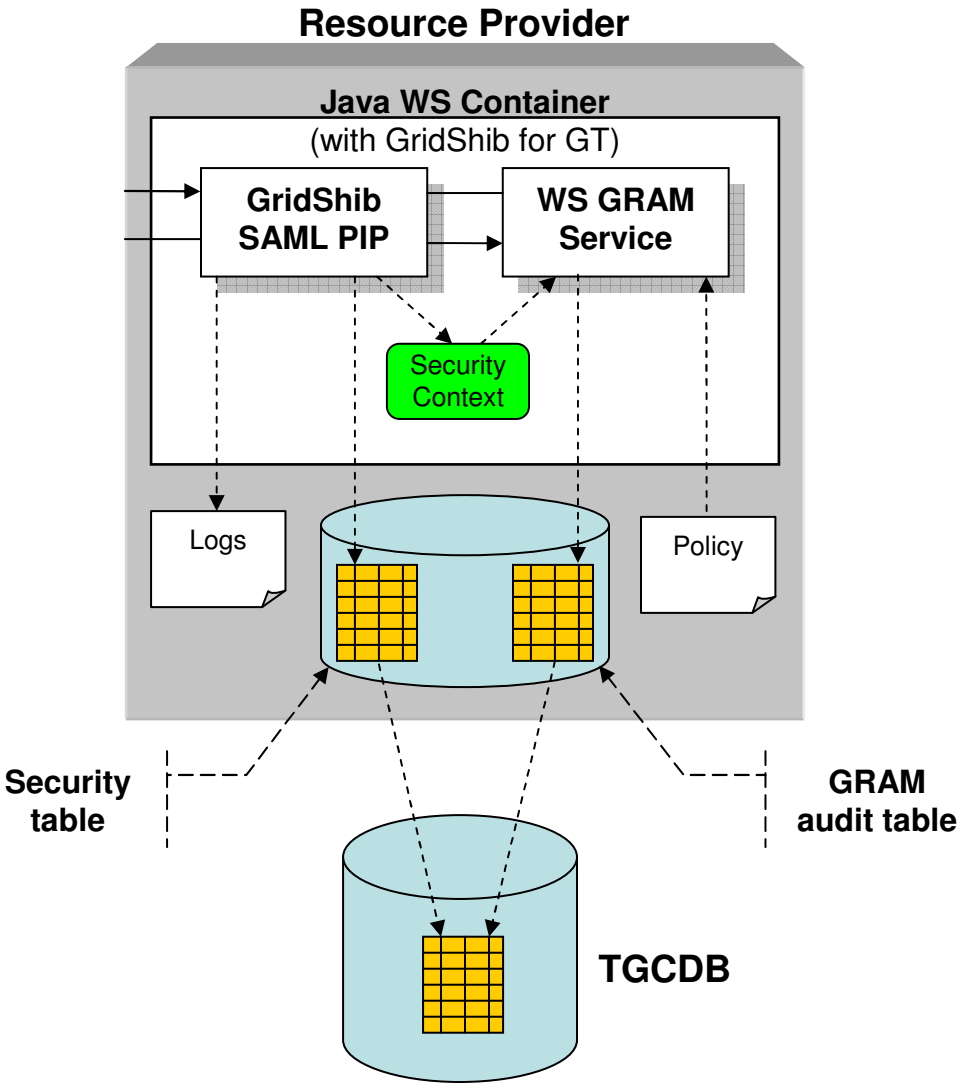
GridShib-enabled Gateway



User Attributes

- Gateway `entityID`:
  - **`https://gridshib.gisolve.org/idp`**
- Subject name identifier:
  - **`trscavo@gisolve.org`**
- Authentication statement
  - authentication method: **`urn:oasis:names:tc:SAML:1.0:am:password`**
  - authentication instant: **`2007-08-02T12:10:34-0400`**
  - IP address: **`10.81.193.244`**
- Attribute statement
  - `isMemberOf` attribute: **`group://gisolve.org/gisolve`**
  - `mail` attribute: **`trscavo@gmail.com`**

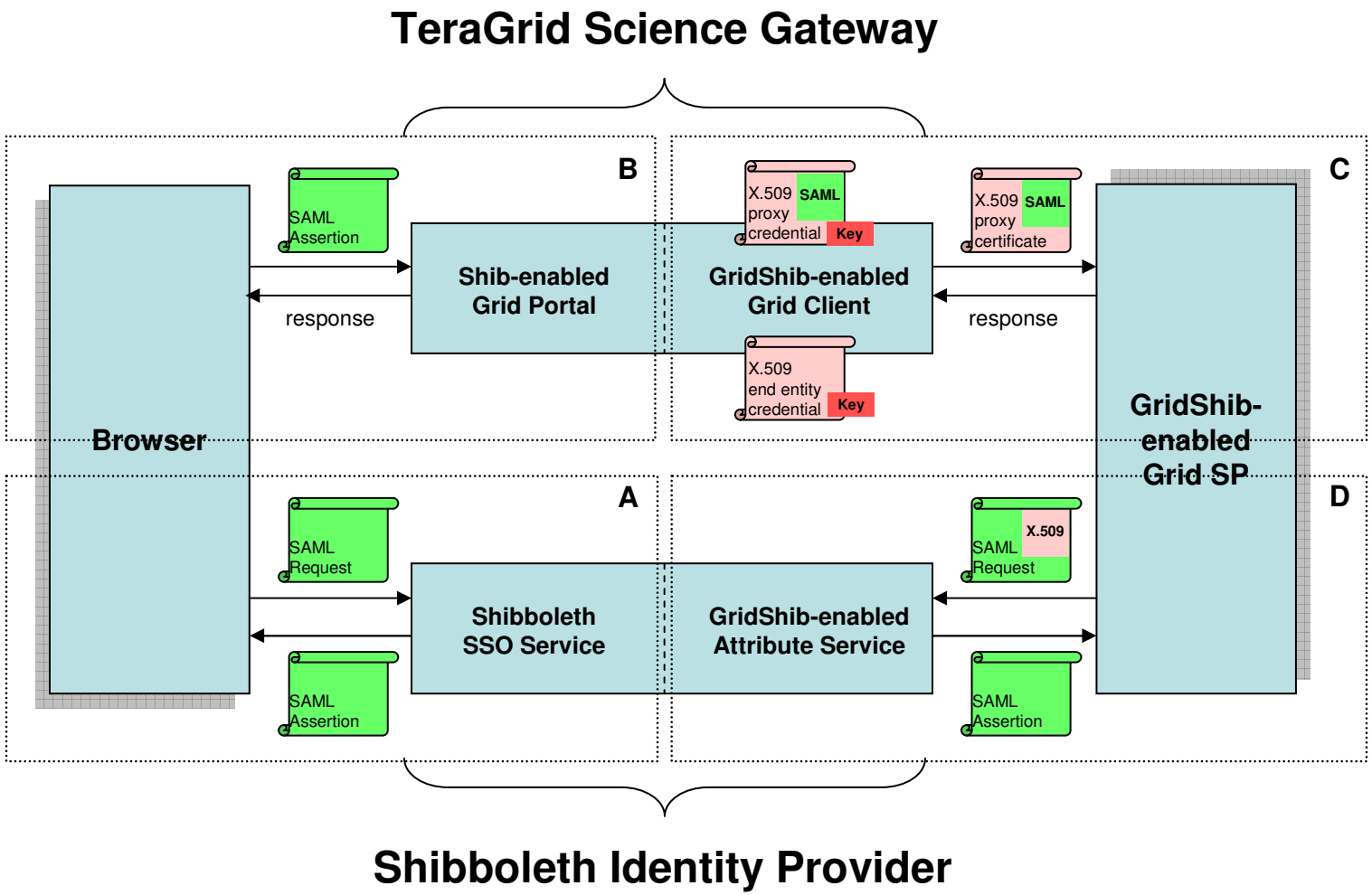
Current Work



TeraGrid Deployment Strategy

1. GridShib SAML Tools at the Gateway
   - http://www.teragridforum.org/mediawiki/index.php?title=Science_Gateway_Credential_with_Attributes
2. GridShib for GT at the RP
   - Integrate GS4GT into CTSS4
3. Evaluate Shibboleth as a browser-facing federated identity solution
   - Planned Shib work at the TG user portal
   - For the most part, Shibboleth has not yet entered the TeraGrid consciousness

Federated Identity Model




Thank you!

Tom Scavo
trscavo@ncsa.uiuc.edu

GridShib
http://gridshib.globus.org/