Internet2 Middleware

in ? minutes

Drinking Kool-Aid From A Fire Hose

Michael R. Gettes
Georgetown University
gettes@Georgetown.EDU
http://www.georgetown.edu/giia/internet2

“Middleware is the intersection of what the Network Engineers and the Application Programmers **don’t** *want to do”*

- Ken Klingenstein

Chief Technologist, Univ. of Colorado, Boulder
Director, Internet2 Middleware Initiative
Lead Clergy, MACE
PS of LC

Internet2 Middleware

If the goal is a PKI, then you need to consider:

- **Identifiers (SSNs and other untold truths)**
- **Identification process ("I & A")**
- **Authentication systems (Kerberos, LDAP, etc)**
- **Lawyers, Policy & Money (lawyers, guns & $$$)**
- **Directories (and the applications that use them)**
- **Certificate Mgmt System (CMS) Deployment**
  - **CA Certficate, Server Certificates, Client Certificates**
- **Authorizations (a real hard problem, Roles, etc)**

Internet2 Middleware

- ***Building Application/System Infrastructure***
- ***What is missing in Internet 1***
- ***Not "Network Security" (wire level)***
- ***Assumes the wire is insecure***
- ***Assumes the Application is insecure***

If security was easy,

everyone would be doing it.

- ***http://middleware.internet2.edu***

MACE

Middleware Architecture Committee for Ed.

IT Architects – meet often – no particular religious affiliations

MACE-DIR – eduPerson, Recipe, DoDHE

MACE-SHIBBOLETH – global AuthN/Z

MACE-PKI → HEPKI (TAG/PAG/PKI-Labs)

MACE-MED – HIPAA, mEduPerson

MACE-WebISO – Web Initial Sign-on

VID-MID – Video Middleware (H.323)

MACE-ochists

RL "Bob" Morgan, Chair, Washington

Steven Carmody, Brown

Michael Gettes, Georgetown

Keith Hazelton, Wisconsin

Paul Hill, MIT

Ken Klingenstein, Colorado

Mark Poepping, CMU

Jim Jokl, Virginia

David Wasley, UCOP

MACE-DIR

Keith Hazelton, Chair, Wisconsin

- eduPerson objectclass
- LDAP-Recipe
- Dir of Dirs for Higher Education (DoDHE)
- Shibboleth project dir dependencies
- Meta Directories – MetaMerge free to HE
- http://middleware.internet2.edu/directories

MACE-DIR: eduPerson 1.0 (1/22/01 release)

- *MACE initiated (Internet2 + EDUCAUSE)*
- *Globally interesting useful attributes*
- *Get community buy-in, must use it also*

eduPersonAffiliation (DoDHE), eduPersonPrincipalName (Shibboleth)

- *"Less is more", how to use standard objectclasses*
- *http://www.educause.edu/eduperson*

MACE-DIR: LDAP-Recipe

DIT, Schema Design, Access Control, Replication, Name population, Good use of LDAP design and features, LDAP configuration, Password Management, eduPerson discussion, DoDHE expectations

http://middleware.internet2.edu (locate LDAP-Recipe)

MACE-DIR: Directory of Directories for Higher Education

Web of Data vs. Web of People

Prototype: April, 2000 (by M. Gettes)

Highly scalable parallel searching

- Interesting development/research problems

Realized the need to:

- Promote eduPerson & common schema
- Promote good directory design (recipe)

Work proceeding – Sun Microsystems Grant

http://middleware.internet2.edu/dodhe

MACE-SHIBBOLETH

Steven Carmody, Brown, Chair

A Biblical pass phrase – "password"

- Get it right or "off with your head"
- Inter-institutional Authentication/Authorization
- Web Authorization of Remote Sites with Local Credentials
- Authentication via WebISO
- October, 2001 – Demo target
- http://middleware.internet2.edu/shibboleth

MACE-WEBISO

Recently Formed

Based on University of Washington "pubcookie" implementation

Carnegie Mellon will likely develop and steward for next 2 years with external funding

JA-SIG uPortal, Blackboard, Shibboleth – will do or are highly likely to do.

http://www.washington.edu/computing/pubcookie

VIDMID
Video Middleware

Recently Formed

Authentication and Authorization of H.323 sessions.

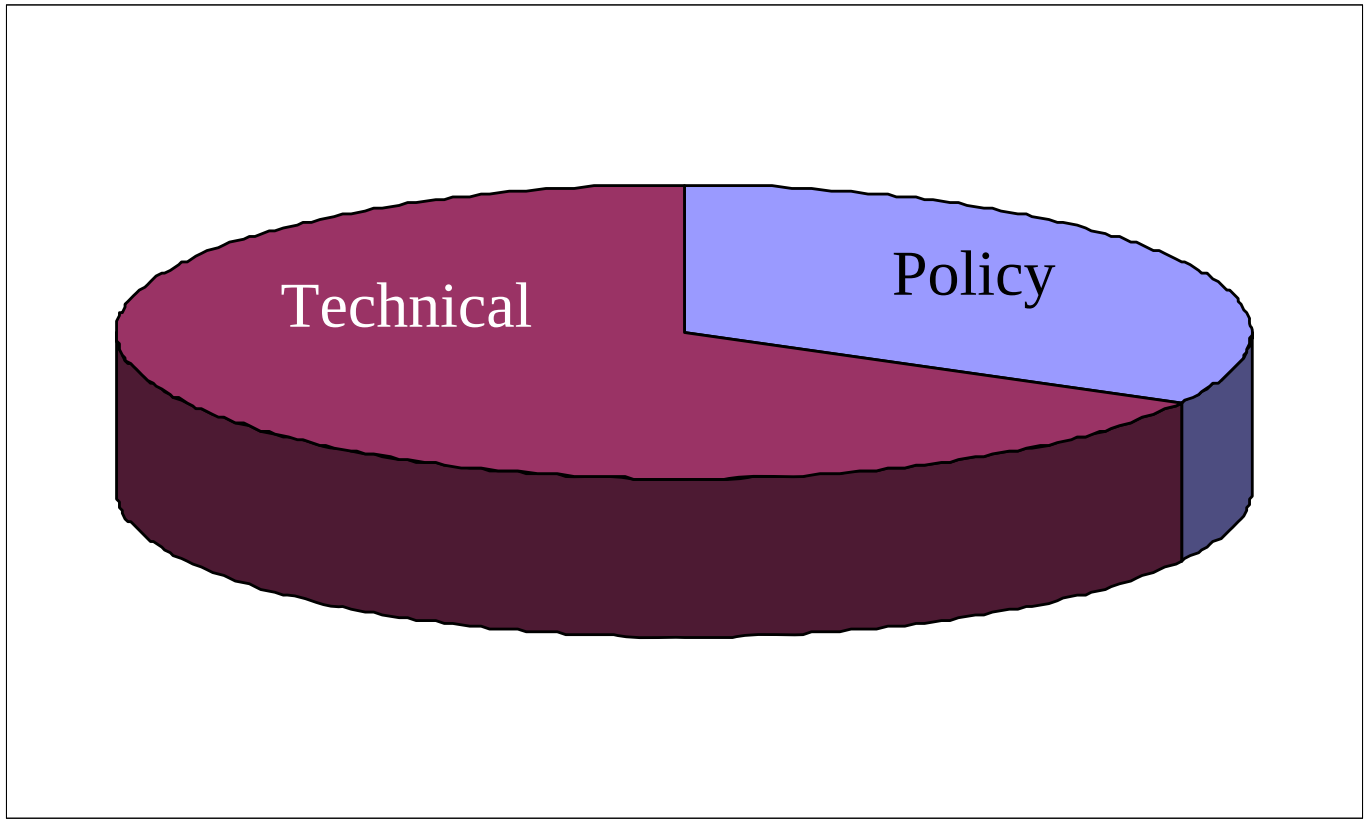
- *Client to Client*
- *Client to MCU*

Directory enabled

- *How to find video enabled people?*
- *What is necessary to describe video capabilities?*

Will likely extend to IP Telephony and so on…

PKI is 1/3 Technical and 2/3 Policy?



HEPKI

TAG – Technical Activities Group

- Jim Jokl, Chair, Virginia
- Mobility, Cert Profiles, etc, etc, lots of techno

PAG – Policy Activities Group

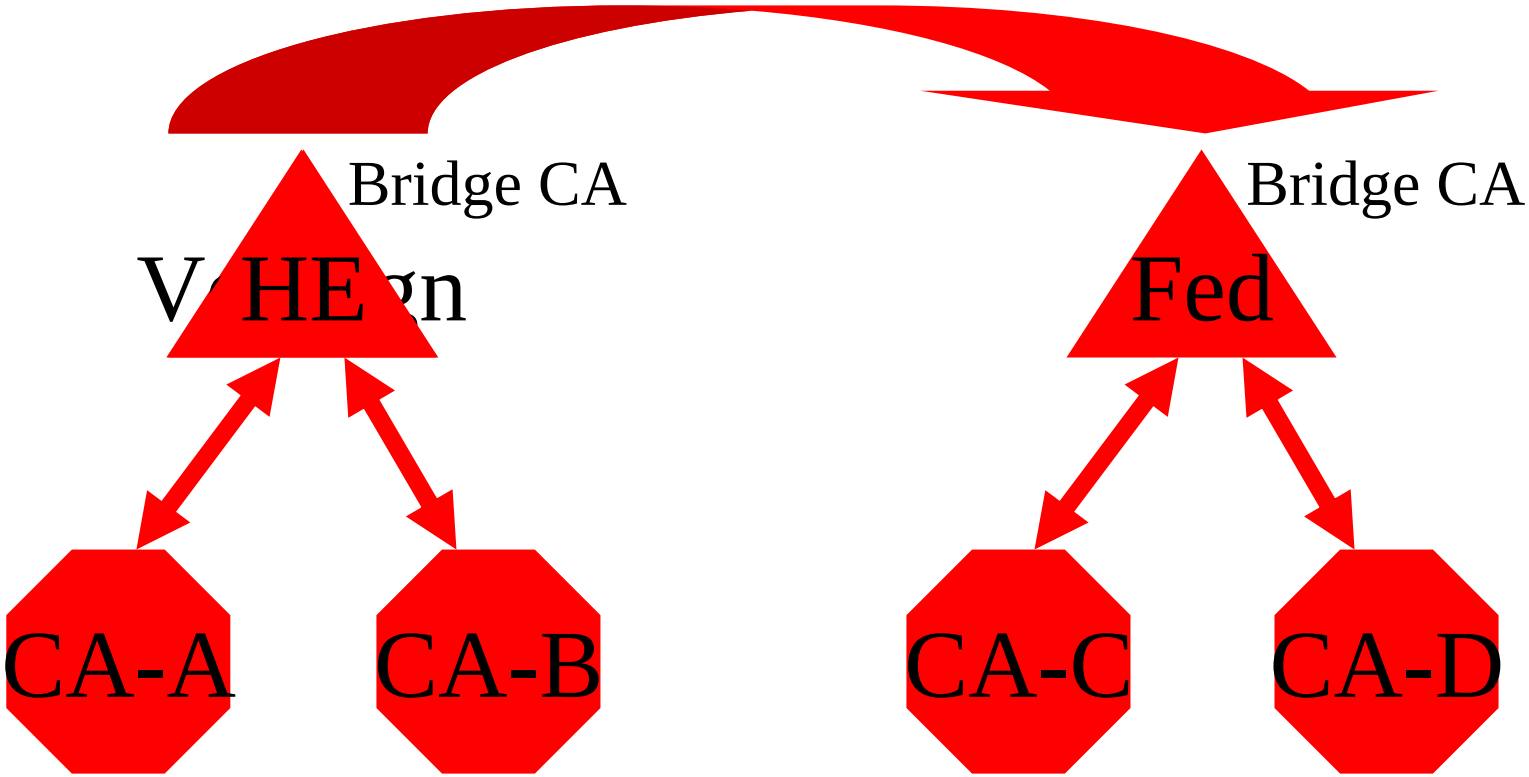
- Default Chair, Ken Klingenstein, Colorado
- Knee-deep in policy, HEBCA, Campus, Subs+RP

PKI Labs (AT&T)– Neal McBurnett, Avaya

- Wisconsin-Madison & Dartmouth
- Industry, Gov., Edu expert guidance

http://www.educause.edu/hepki

Bridge CA and Trust Paths



Bridge CAs

- *Higher Education Bridge CA – FBCA peering*
- *We have a draft HEBCA CP (Net@EDU PKI WG) FBCA Compatible*
- *How many HEBCAs? (EDUCAUSE!)*
- *Do we really understand PKI implementations with respect to policy needs? (proxy certificates, relying party agreements, name constraints, FERPA, HIPAA, who eats who?)*
- *BCA seems to be the most promising perspective. Will each person be a BCA?*
- *Does ALL software (Client/Server) need to be changed?*
- *Mitretek announces new BCA deployment model 2/15/2001*
  - Scalable & deployable
  - Server plug-ins make client changes less likely

domainComponent (DC=) Naming

- *Traditional X.500 naming:*

cn=Michael R Gettes, ou=Server Group, ou=UIS, o=Georgetown University, c=US

- *domainComponent (DC) naming:*

uid=gettes,ou=People,dc=georgetown,dc=edu

  - HEPKI is issuing guidance and advice on DC= naming

Attributes for PKI

Store them in a Certificate?

- Attributes persist for life of Certificate
- No need for Directory or other lookup
  - The Certificate itself becomes the AuthZ control point

Store them in a Directory?

- Very light-weight Certificates
- Requires Directory Access
- Long-term Certificate, Directory is AuthZ control point.

How many Certificates will we have?

Pseudonymous Certificates

INTERNET2™

We’re Building A

“Bridge Over The River PKI”

A word about “Portals”

Portals: Authentication

- *Security is not easy*

  if it was, then everyone would be doing it. ☺

- *Applications **should not** handle authentication*
  - Don't assume you will have access to passwords at the portal

- *The portal is YAA (yet another application)*

  but portals have web servers to do the dirty work

  portals can trust the web server to authenticate

  and pass "identity" on to the portal

Portals: Authorization

- *Security is not easy*

  if it was, then everyone would be doing it. ☺

- *Applications **should** handle authorization*

- *The portal is YAA (yet another application)*

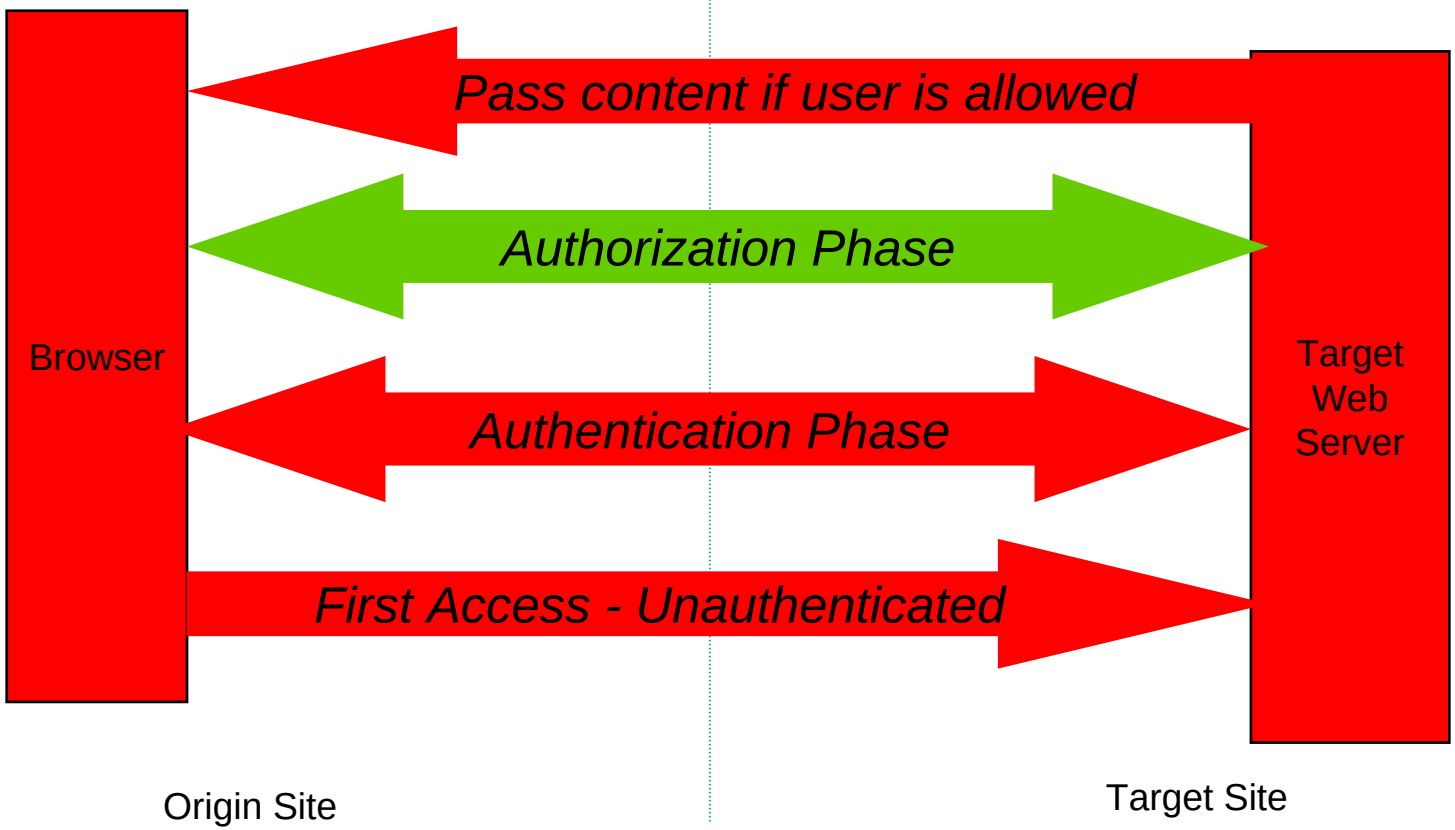
  Portals can decide access on their own by consulting local and remote services to determine eligibility then grant/deny based on response or otherwise by whim.

Shibboleth Update

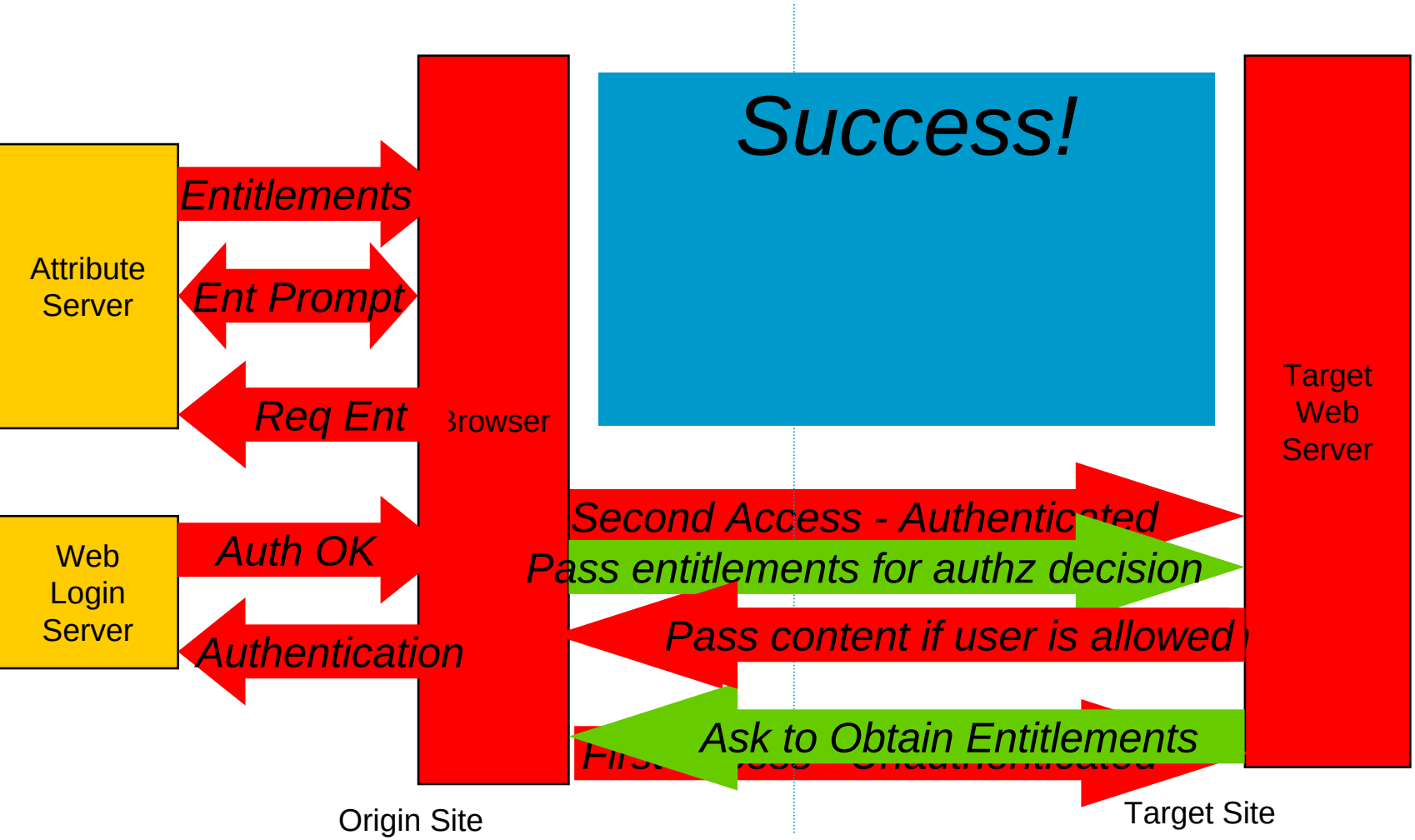
February, 2001

Steven Carmbody, Brown University
Michael R. Gettes, Georgetown University

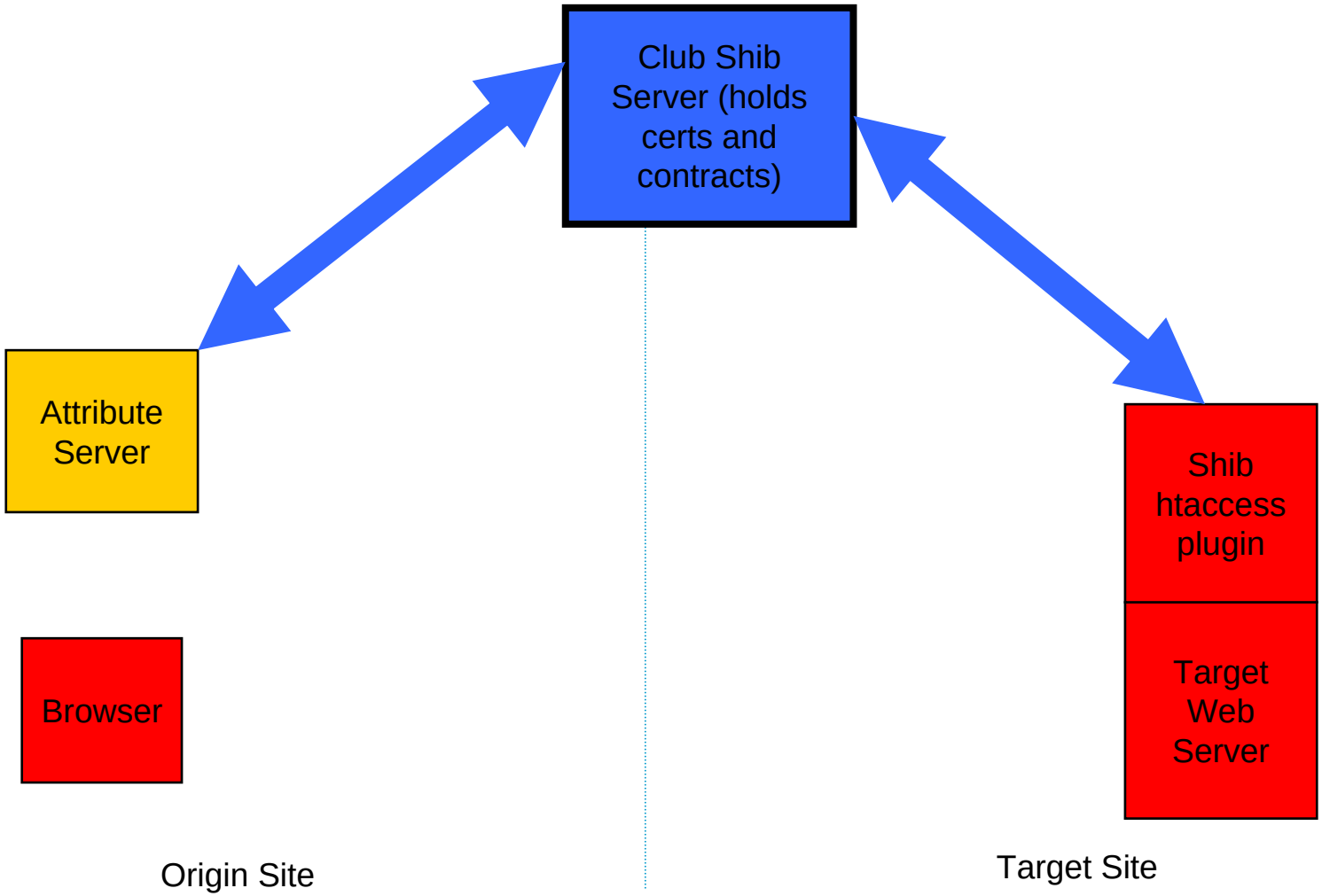
Shibboleth Architecture Concepts - High Level



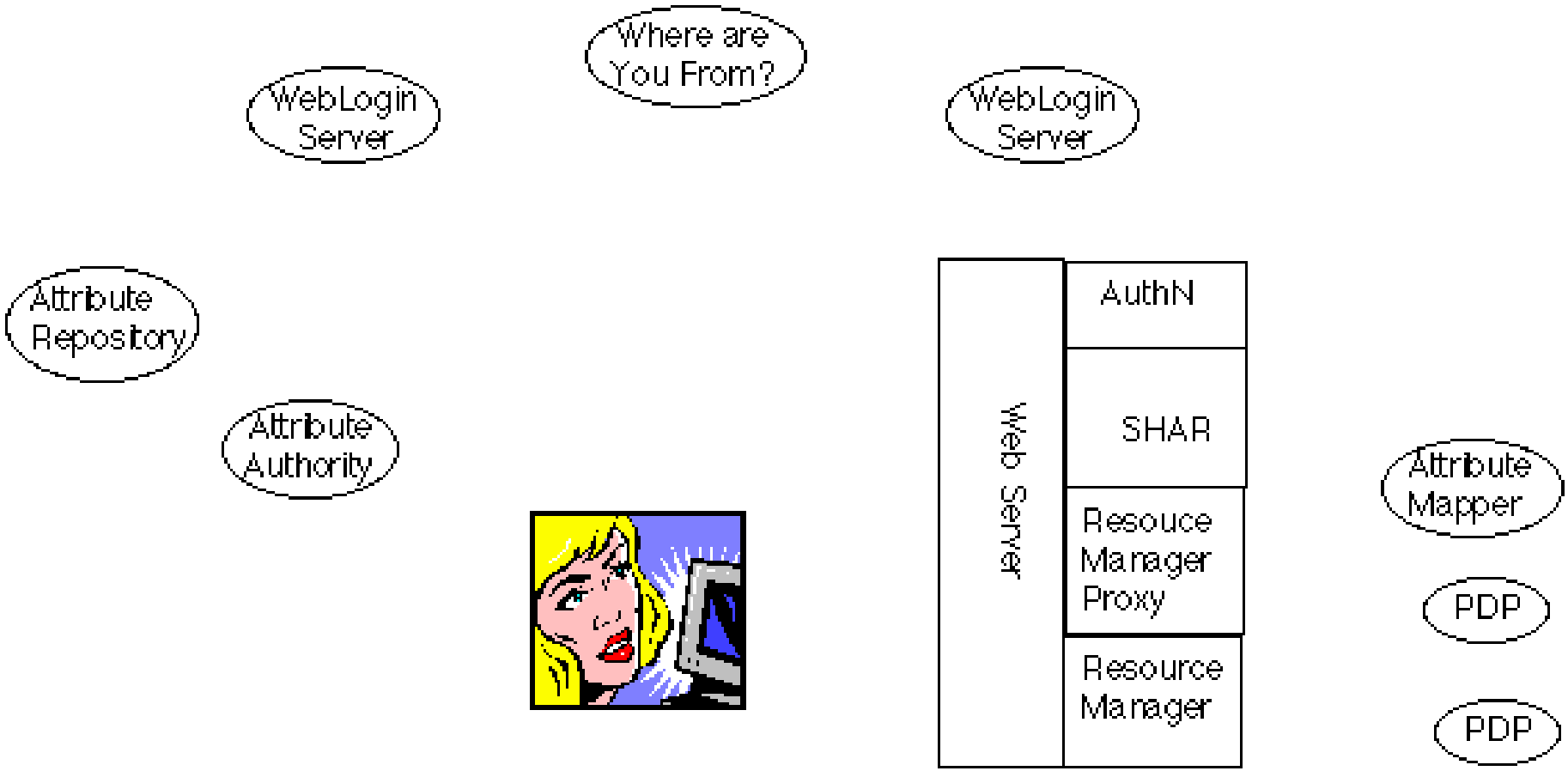
Shibboleth Architecture Concepts (detail)



Shibboleth Architecture Concepts #1 (managing trust)



Shibboleth Components



Descriptions of services

local authn server - assumed part of the campus environment

web sso server - typically works with local authn service to provide web single sign-on

resource manager proxy, resource manager - may serve as control points for actual web page access

attribute authority - assembles/disassembles/validates signed XML objects using attribute repository and policy tables

attribute repository - an LDAP directory, or roles database or….

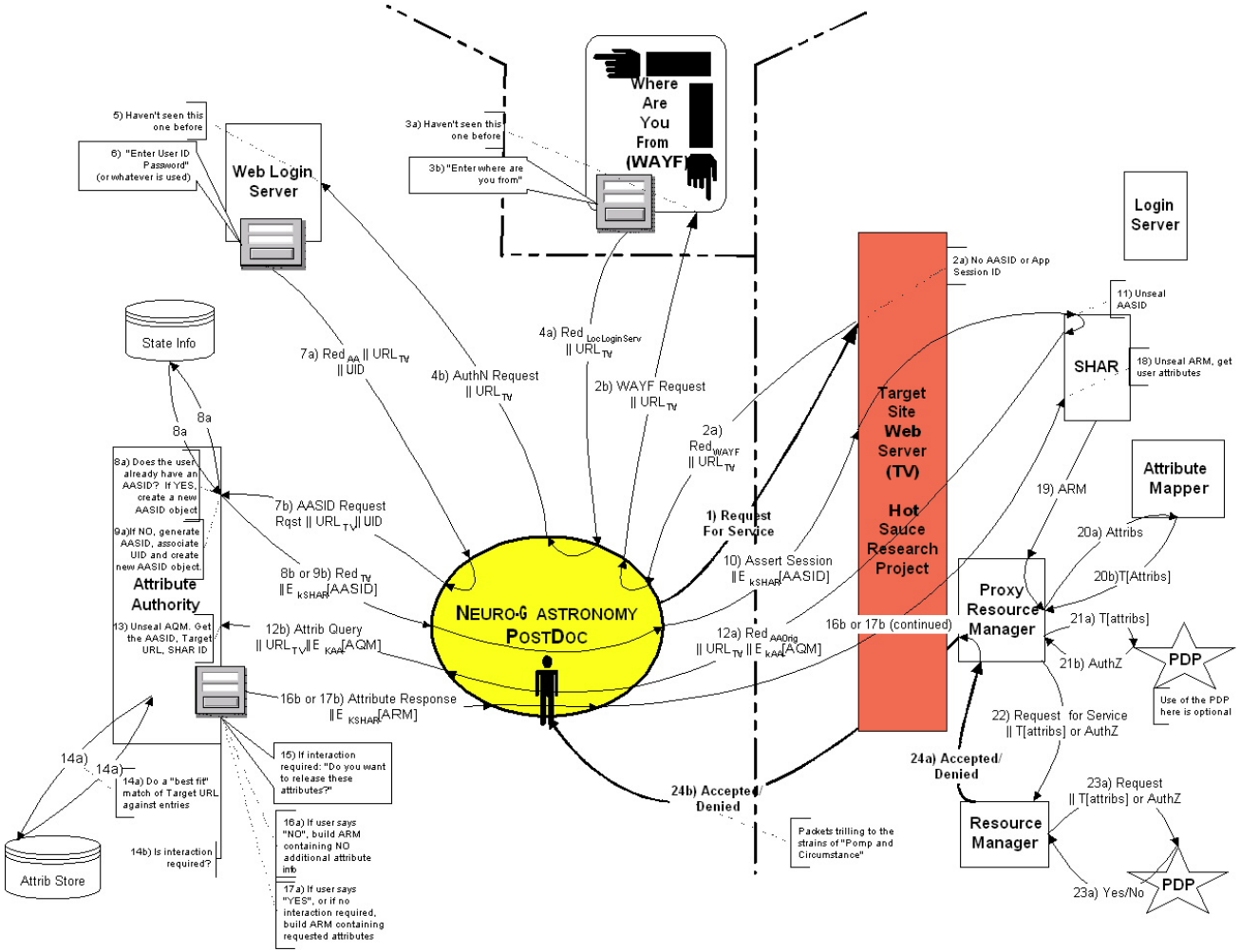
Where are you from service - one possible way to direct external users to their own local authn service

attribute mapper - converts user entitlements into local authorization values

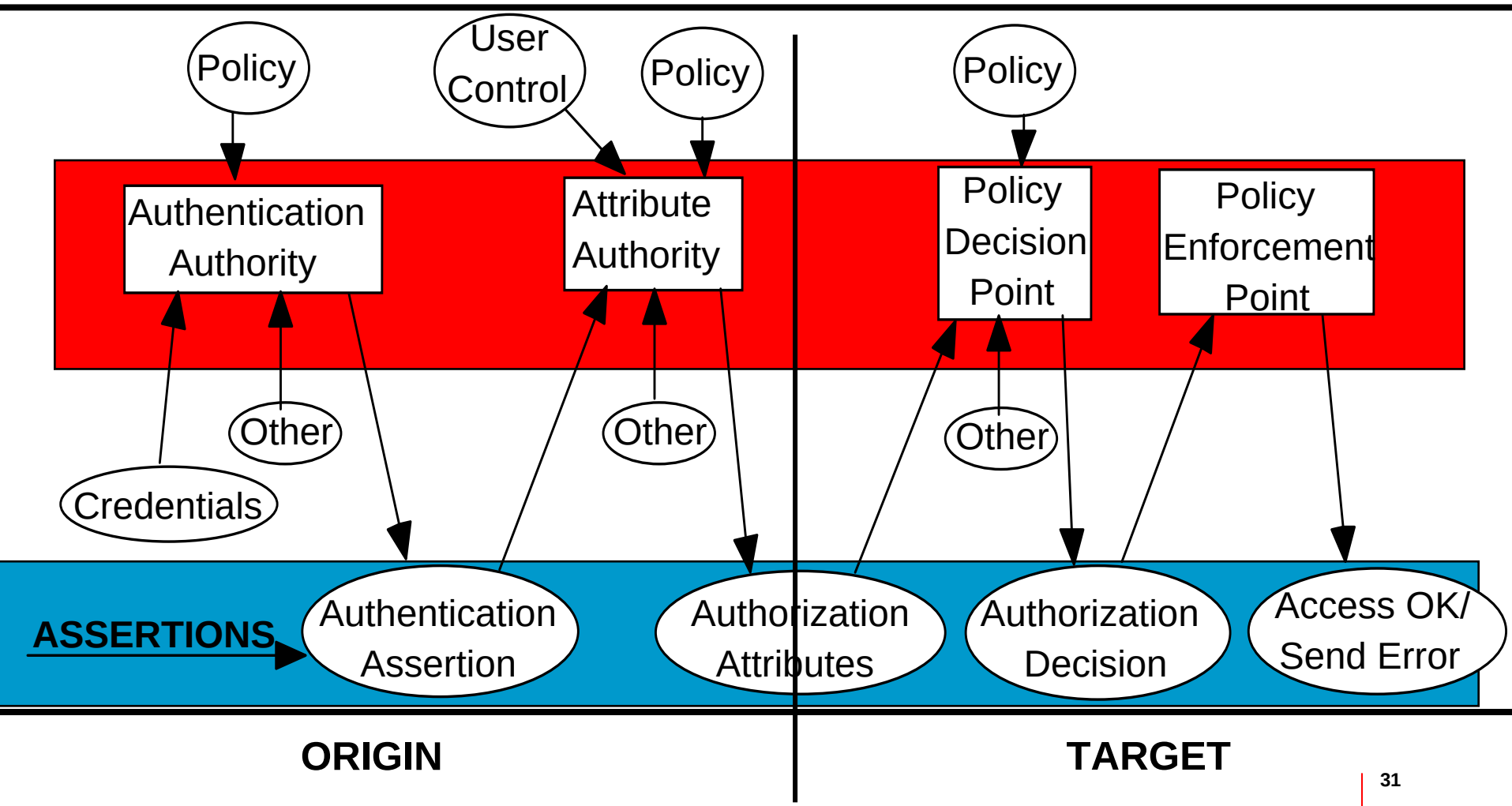
PDP - policy decision points - decide if user attributes meet authorization requirements

SHAR - Shibboleth Attribute Requestor - used by target to request user attributes

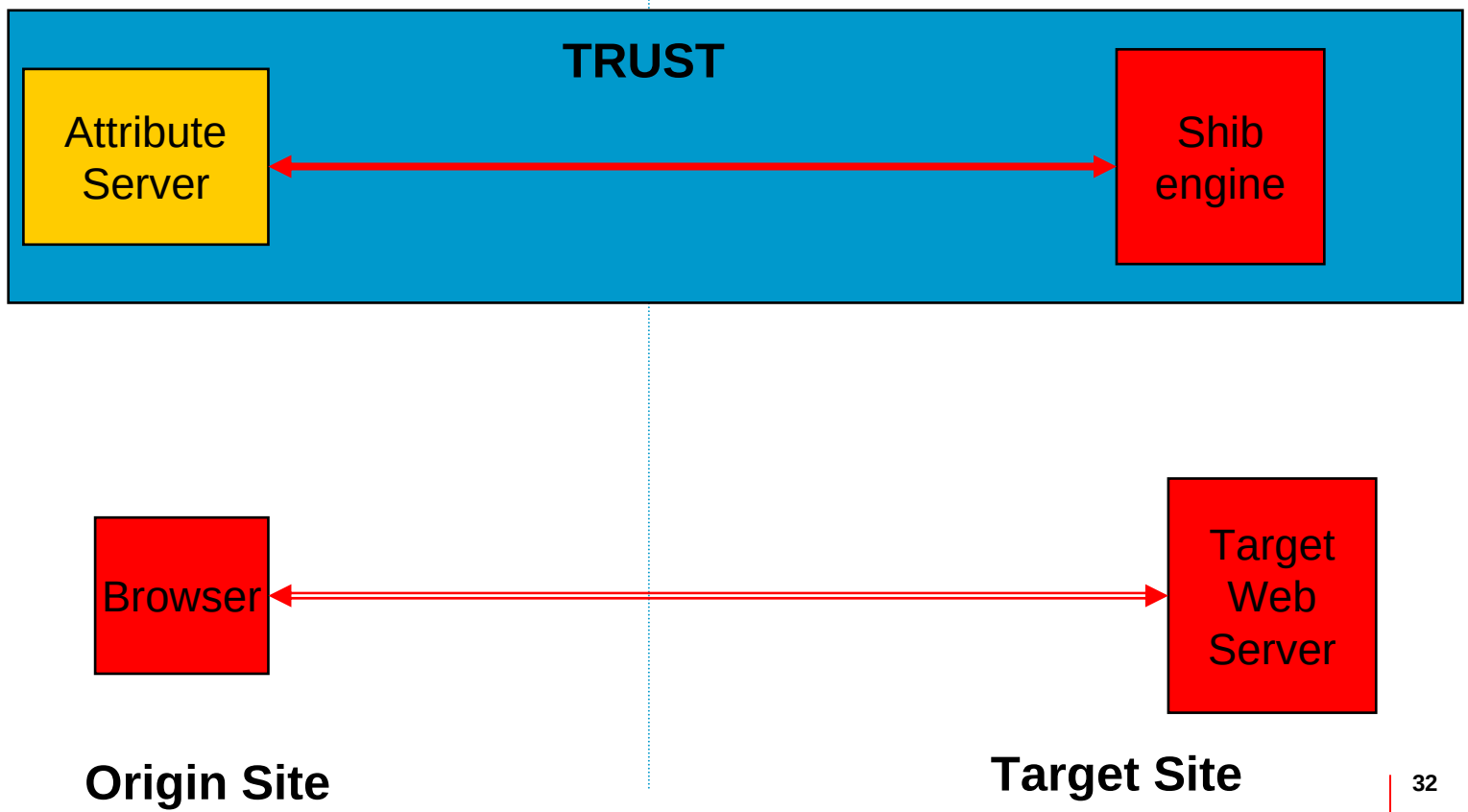
Shibboleth Flows Draft



Component Relationship Model



Shibboleth Architecture -- Managing Trust

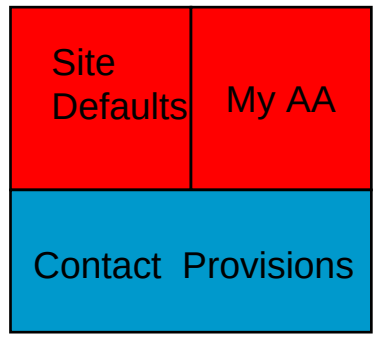


Personal Privacy

Web Login Server provides a pseudononymous identity

An Attribute Authority releases Personal Information associated with that pseudnonymous identity to site X based on:

- Site Defaults
  - Business Rules
- User control
  - myAA
- Filtered by
  - Contract provisions

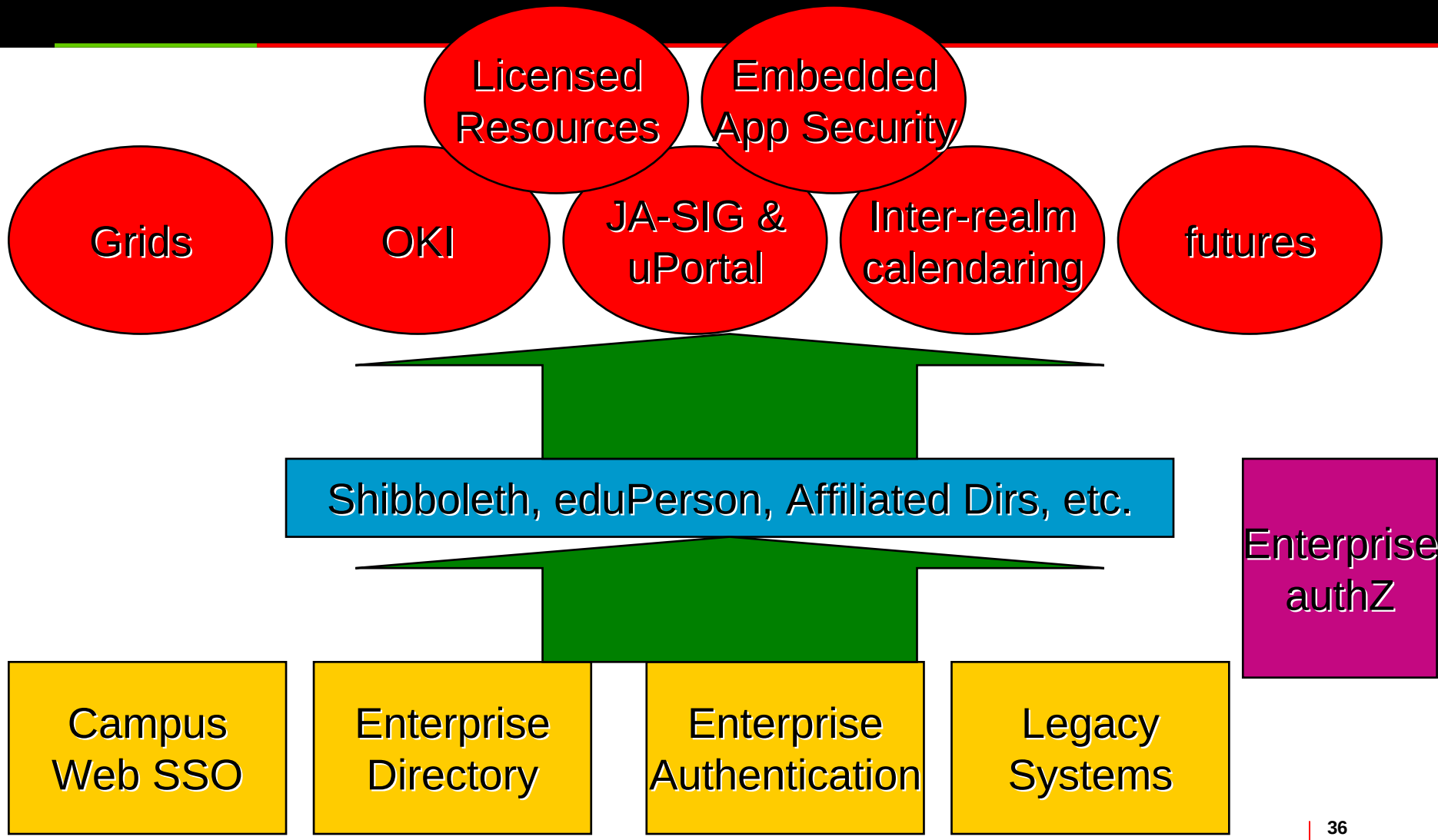


Browser User

Middleware Marketing

Drivers of Vapor Convergence

Middleware Inputs & Outputs



Got Directory?

Authentication: Overall Plan @ Georgetown

Currently, Server-Side PKI self-signed

Best of all 3 worlds

- LDAP + Kerberos + PKI
  - LDAP Authentication performs Kerberos Authentication out the backend. Jan. 2001 to finish iPlanet plug-in.
    - Credential Caching handled by Directory.
    - Cooperative effort – Georgetown, GATech, Michigan
  - All directory authentications SSL protected. Enforced with necessary exceptions
- Use Kerberos for Win2K Services and to derive X.509 Client Certificates
- One Userid/Password (single-signon vs. FSO)

Directories *are* part of the I in PKI

Directory (October, 1999 @ Georgetown)

- Centralized, automated Name Space
- VERY carefully controlled
  - Users modify very little
  - Priv'd access highly restricted
- Control considered necessary step for PKI to **trust** the directory
- Eventually, client, server and other certs/CRLs will be published in the directory.

Are Directories part of the I in PKI?

Michigan (Kx509), Columbia

- Short-lived Certificates
- Avoids CRL and Directory Publications

MIT

- 1 year certs, but people can get all they need using Kerberos Authentication

Site Profile
dc=georgetown,dc=edu

Netscape/iPlanet DS version 4.11

- 2 Sun E250 dual cpu, 512MB RAM

75,000 DNs (25K campus, others = alums + etc)

Distinguished names: uid=xxx,ou=people

iDS pre-op plugin (by gettes@Princeton.EDU)

- Authentication over SSL; Required

1 supplier, 4 consumers

Applications @ G’town

iPlanet Messaging Server 4.15 (IMAP)

- WebMail profile stored in directory

Mail routing with Sendmail 8.10 (lists also)

Apache & iPlanet Enterprise web servers

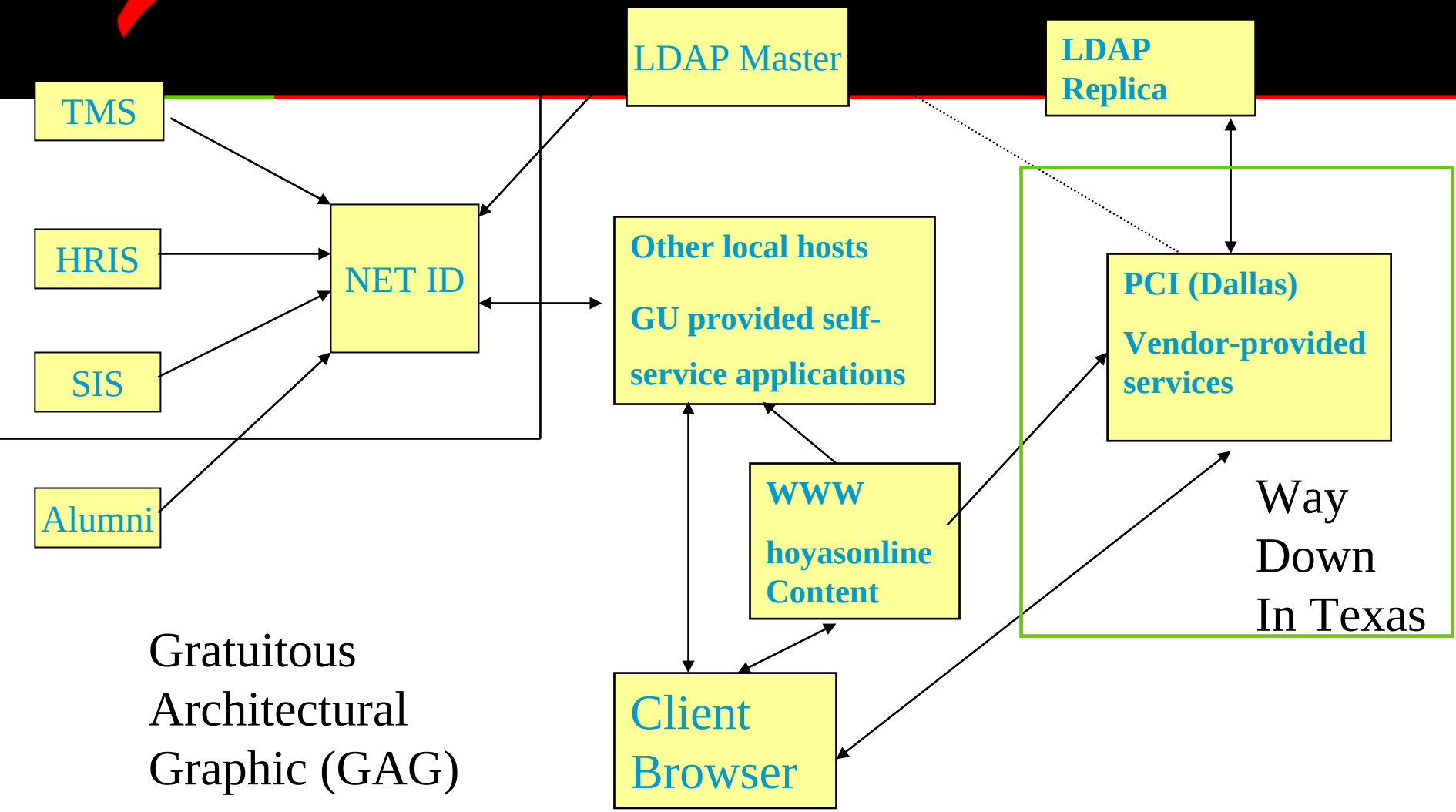
Blackboard CourseInfo Version 5 Level 3

Whitepages: Directory Server GateWay

CorporateTime Calendaring

Alumni HoyasOnline Service w/ PCI (Dallas)

- External Vendor Collaboration & Development



Gratuitous Architectural Graphic (GAG)

Applications @ G'town

RADIUS

- Remote Access mgmt: Modem pools, VPN
- Resource Management/Authorization
  - Oracle 8i has RADIUS abilities

Person Registry

- Manages namespace; MVS based for now

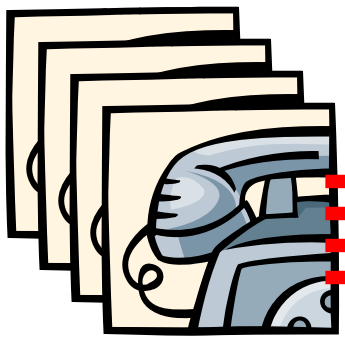
PerLDAP: very powerful. JAVA as well.

Dynamic/Static Groups (authZ, lists, …)

RADIUS + LDAP

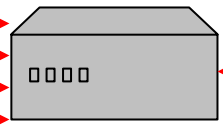
IN

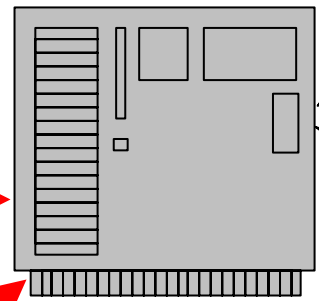
202-555-1110



Dialup Users

NAS (terminal server)





RADIUS server

CalledId from NAS is mapped to guRadProf

LDAP Filter is: guRadProf = 2025551110 + NetID = gettes

Directory Server

Netid = gettes
guRadProf = 2025550001
guRadProf = 2025551110
guRadProf = OracleFin

Applications (Continued)

Specialized support apps

- Self service mail routing
- Help Desk: mail routing, password resets, quota management via iPlanet DSGW
- Change password web page

Applications (Continued)

Georgetown Netscape Communicator Client Customization Kit (CCK).

- Configured for central IMAP/SSL and directory services.
- Handles versions of profiles. Poor man's MCD

Future: more apps! Host DB, Kerberos integration, win2k/ad integration?, Oracle RADIUS integration, Automatic lists, Dynamic/static Groups, Top-Secret, VoIP

Further Integration: Blackboard, CorporateTime Calendaring, Cognos …