Akenti: An Approach to Multi-Stakeholder Resource Access Control*

(An Application of Public-key Infrastructure and Digitally Signed Certificates)

*William E. Johnston***, *Abdelilah Essiari, Gary Hoo, Keith Jackson,*
Srilekha Mudumbai, and Mary Thompson
Information and Computing Sciences Division
Ernest Orlando Lawrence Berkeley National Laboratory
University of California

*This work is supported by the Director, Office of Energy Research, Office of Computation and Technology Research, Mathematical, Information, and Computational Sciences Division, of the U. S. Department of Energy under Contract No. DE-AC03-76SF00098 with the University of California. See http://www-itg.lbl.gov/Security/Akenti for more information.
**wejohnston@lbl.gov (510-486-5014), mudumbai@george.lbl.gov, mrt@george.lbl.gov – http://www-itg.lbl.gov

Access Control for Widely Distributed Systems

Motivation:

Our scientific environment involves

- **multi-user instruments at national facilities**
- **widely distributed supercomputers and large-scale storage systems**
- **data sharing in restricted collaborations**
- **network-based multimedia collaboration channels**

and these facilities, collaborations, and stakeholders are diffuse – geographically distributed and multi-organizational.

These circumstances require

- **distributed management –because the principals and resources are dispersed organizationally**
- **distributed access control –because the resources and users are dispersed geographically**

Use a Well Understood Approach as a Model

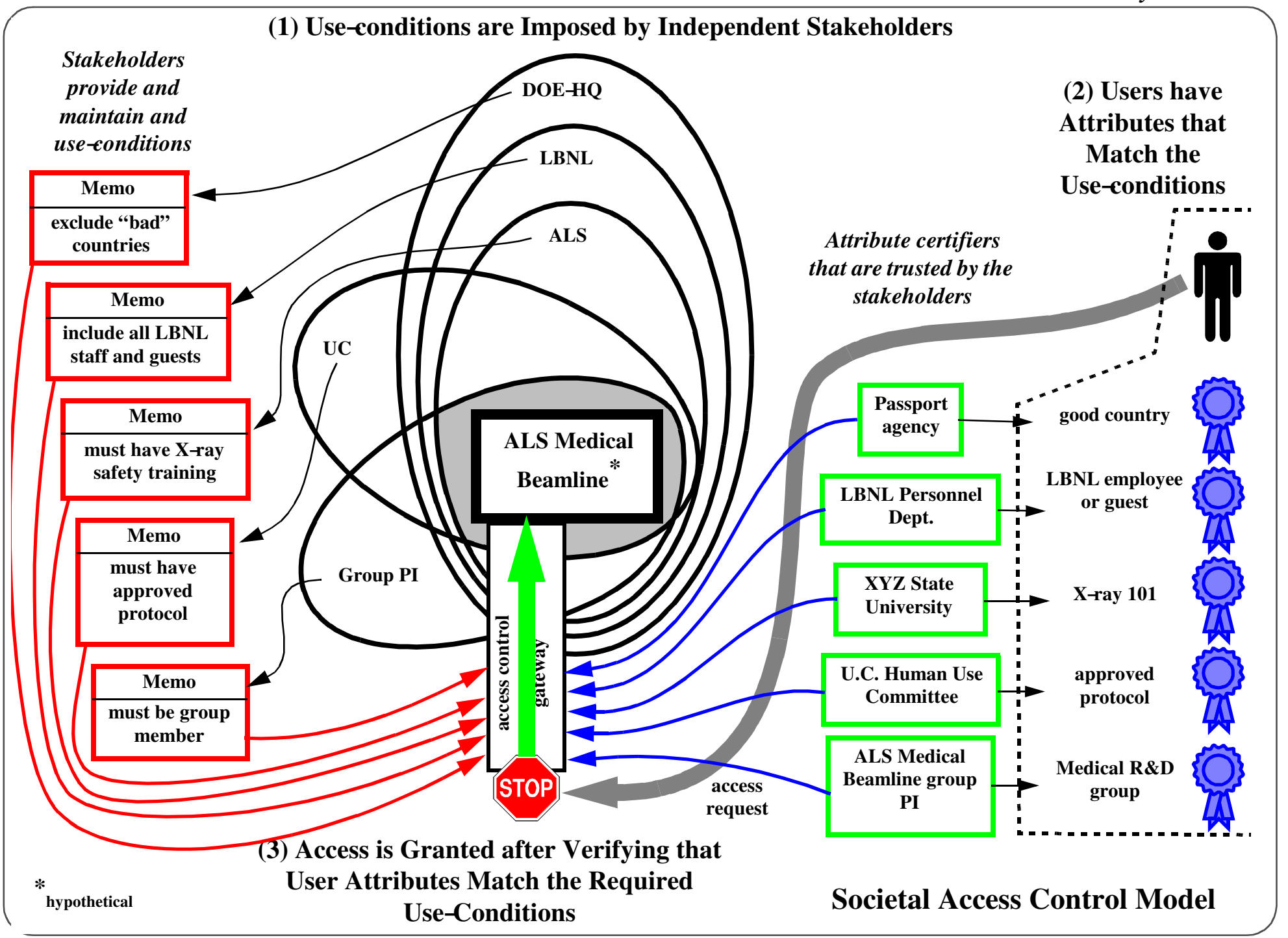
Stakeholders are identified by (usually) written policy

Representations of authority ("use-conditions") are made by written, signed procedures, memoranda, etc.

The required use-conditions are satisfied by a set of attributes: organizational membership, training, etc.

Who and/or what can attest to users' satisfaction of the use-conditions is established by policy: e.g. a token issued by a personnel department, a certificate of training issued by an accredited school, etc.

Credential checking is usually based on an operational authority that compiles a list of stakeholder use-conditions and then validates the users' attributes against this list


(1) Use-conditions are Imposed by Independent Stakeholders
Stakeholders provide and maintain and use-conditions
DOE-HQ
LBNL
ALS
UC
Group PI
Memo
exclude "bad" countries
Memo
include all LBNL staff and guests
Memo
must have X-ray safety training
Memo
must have approved protocol
Memo
must be group member
ALS Medical Beamline *
access control
gateway
STOP
(2) Users have Attributes that Match the Use-conditions
Attribute certifiers that are trusted by the stakeholders
Passport agency
LBNL Personnel Dept.
XYZ State University
U.C. Human Use Committee
ALS Medical Beamline group PI
good country
LBNL employee or guest
X-ray 101
approved protocol
Medical R&D group
access request
(3) Access is Granted after Verifying that User Attributes Match the Required Use-Conditions
* hypothetical
Societal Access Control Model

All of the attributes that match use-conditions are likely to be packaged into a "capability" –a single document (e.g. a "license" or badge) that names the user, and perhaps the resource and the range of permitted actions

The access control enforcer –a door guard, the experiment PI, etc. – typically just validates the capability (e.g., checks the license) when access is requested

This general societal model provides us with the framework for an on-line architecture that accomplishes the same sort of access control for on-line resources.

Overall Goals

On-line access control for the scientific environment must provide:

Secure sharing of resources in a way the reflects currently accepted practice and principles:

- **stakeholders independently make assertions about resource use**
- **trusted third-parties certify user attributes required for the use-conditions**
- **authenticated users that posses the required attributes easily gain access**
- **the level of credential checking (and security) is determined by the nature of the resource being protected**

Dynamic and easily used mechanisms for generation, maintenance, and distribution of the access control information

- **those that make assertions (e.g. establish the use-conditions or attest to user attributes) must be able to do so within their own working environment (usability!)**

Strong assurances that use-conditions are met

- **access decisions must be made based on assured information and then enforced by strong security services**

A policy-neutral mechanism

- **policy is a reflection of agreements among humans**
- **represent policy by assured "pointers" –digitally signed documents containing keywords and values (the type and name of the underlying policy agreement)**
- **access control is by data driven certificate validation and analysis**

Meta-Goals

Policy free X.509

Separate access control policy from security mechanisms

Extensible "certificate" analyzer

Easily integrated with applications

Generalized service for "digital contracts" (X9.45)

General Approach

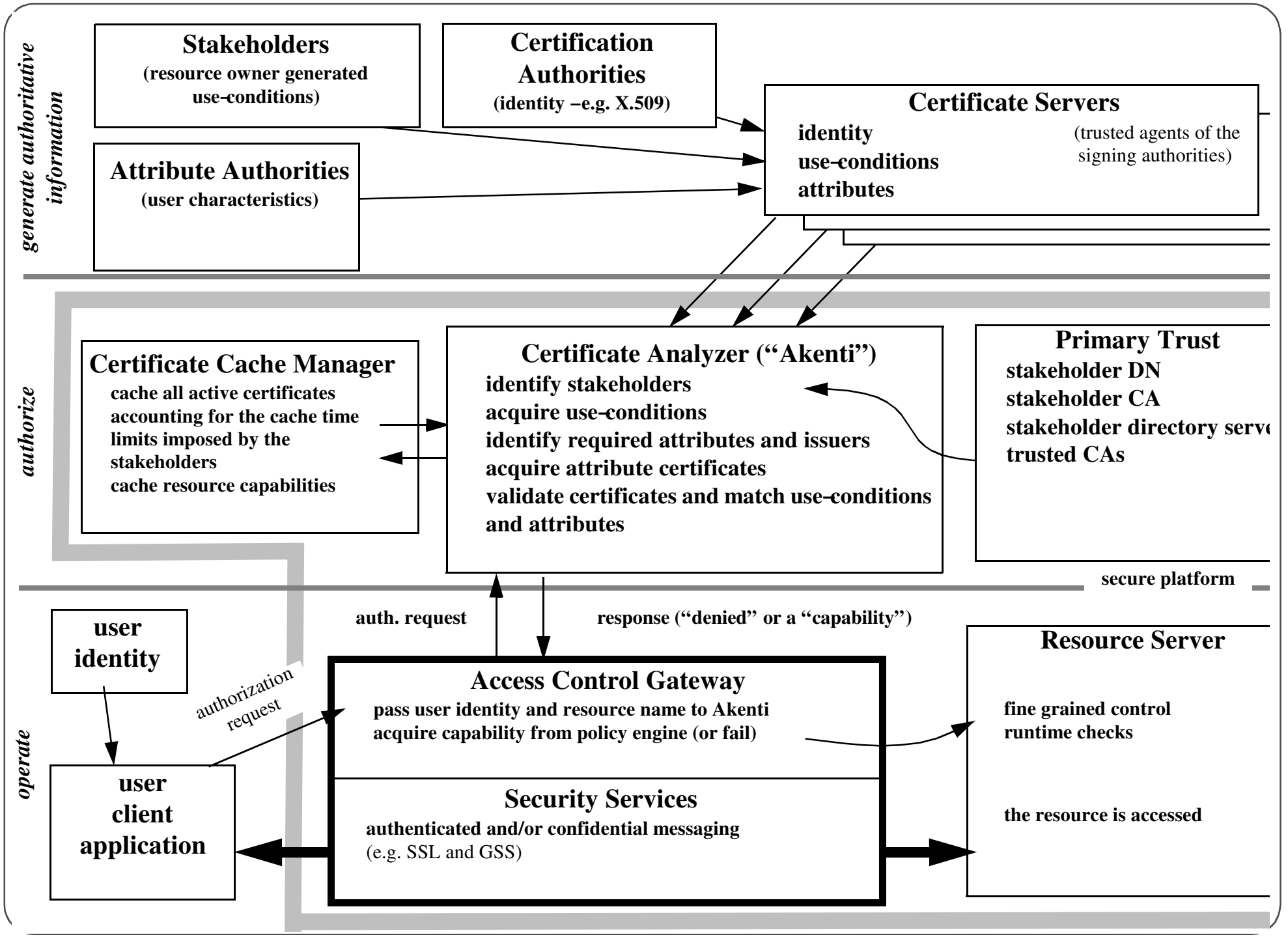
Stakeholders are associated with resources by trusted third parties (currently in configuration files associated with the resource)

All other "trust" is explicit

- **trusted CAs are represented by their names and public keys**
- **certificate issuers are represented by their names and CAs**

Akenti is basically a data driven certificate analyzer

- **user identity and resource identity are presented**
- **stakeholders are identified**
- **use-conditions are collected and verified**
- **required attributed are located and verified**
- **result is packaged as a "capability" and passed to the resource access control gateway**


generate authoritative information
Stakeholders
(resource owner generated use-conditions)
Certification Authorities
(identity –e.g. X.509)
Attribute Authorities
(user characteristics)
Certificate Servers
identity
use-conditions
attributes
(trusted agents of the signing authorities)
authorize
Certificate Cache Manager
cache all active certificates
accounting for the cache time limits imposed by the stakeholders
cache resource capabilities
Certificate Analyzer ("Akenti")
identify stakeholders
acquire use-conditions
identify required attributes and issuers
acquire attribute certificates
validate certificates and match use-conditions and attributes
Primary Trust
stakeholder DN
stakeholder CA
stakeholder directory serv
trusted CAs
secure platform
auth. request
response ("denied" or a "capability")
operate
user identity
authorization request
user client application
Access Control Gateway
pass user identity and resource name to Akenti
acquire capability from policy engine (or fail)
Security Services
authenticated and/or confidential messaging
(e.g. SSL and GSS)
Resource Server
fine grained control
runtime checks
the resource is accessed

Use-condition certificates

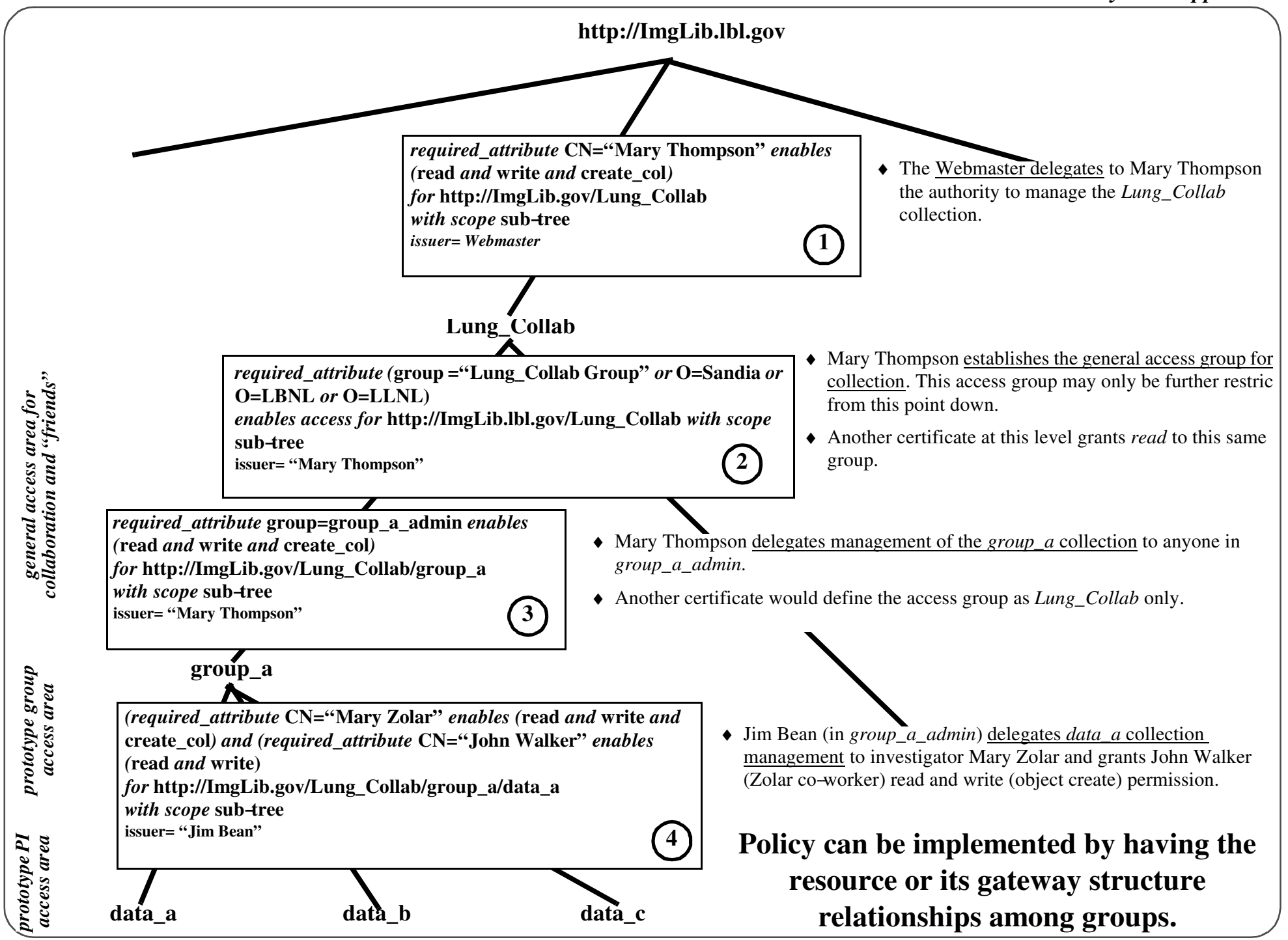
- **allow stakeholders to impose their requirements in a "natural and convenient" way –by representing them as digitally signed documents that are generated, maintained, and distributed in the stakeholder's "local" (working) environment**
- **use-conditions are expressed as named attributes having required values (usually "membership in named groups")**
- **may include "scope" –to support a hierarchical policy model –and lists of permitted actions (vis a vis a particular resource)**
- **can also be expressed as required values for components of DN**

Attribute certificates

- **attribute certificates assign characteristics to DNs (i.e. named attribute has value X –frequently thought of as placing DN in named group)**
- **issued by trusted third parties (named in use-condition certificate) from their working environment, like use-condition certificates**
- **can carry auxiliary information that has meaning for resource access control gateway (e.g. permitted operations, objects to access, valid times of day, etc.)**
- **many namespace problems –in general, will probably have to establish an authoritative mapping function**

Identity

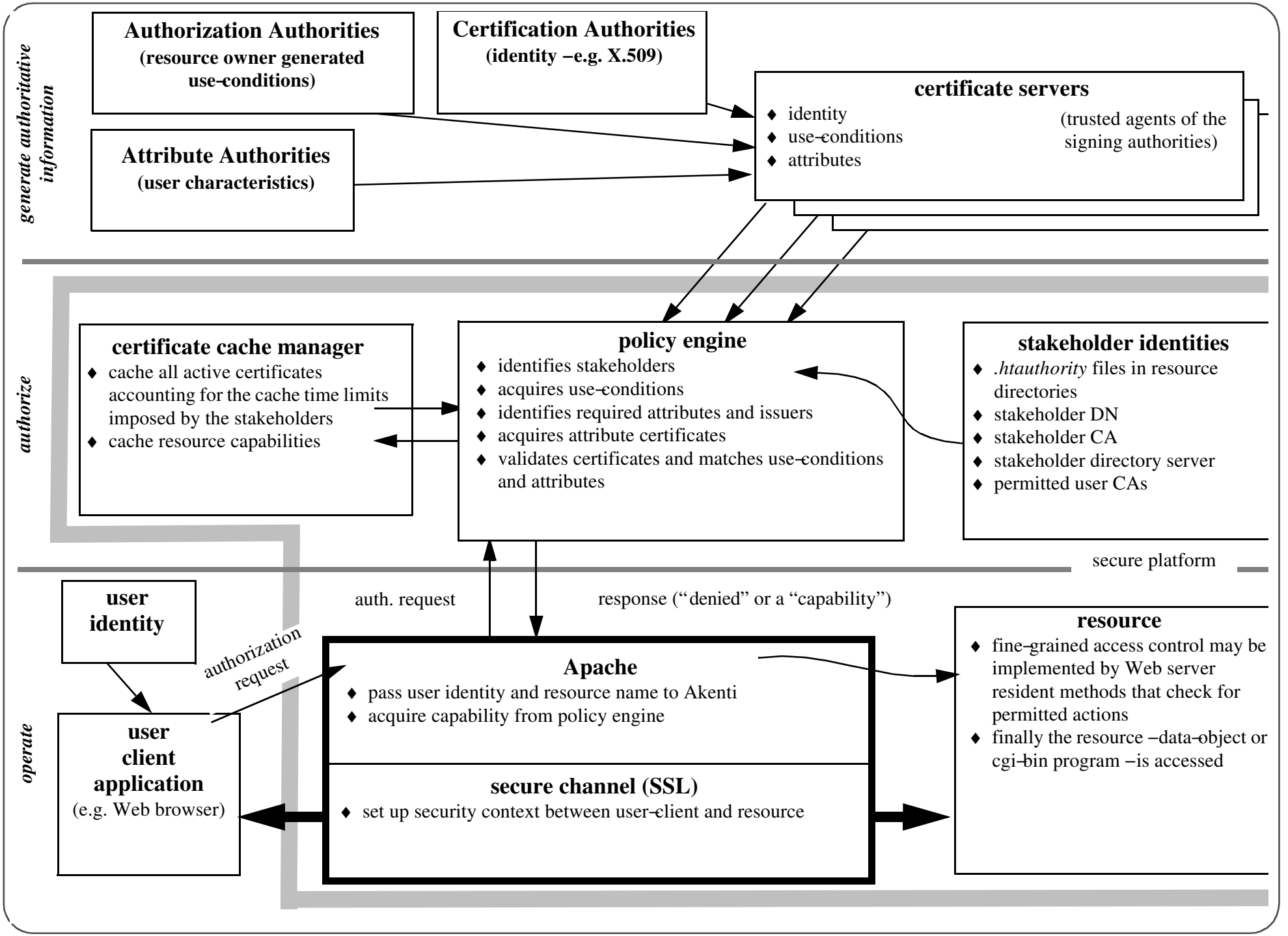
- **standard X.509 certificates and Certification Authority infrastructure are used for identifying and authenticating various entities**
- **X.509 cert. acts as attribute certificate when requirement is DN component**


http://ImgLib.lbl.gov
required_attribute CN="Mary Thompson" enables (read and write and create_col) for http://ImgLib.gov/Lung_Collab with scope sub-tree
issuer= Webmaster
1
The Webmaster delegates to Mary Thompson the authority to manage the Lung_Collab collection.
Lung_Collab
required_attribute (group ="Lung_Collab Group" or O=Sandia or O=LBNL or O=LLNL) enables access for http://ImgLib.lbl.gov/Lung_Collab with scope sub-tree
issuer= "Mary Thompson"
2
Mary Thompson establishes the general access group for collection. This access group may only be further restric from this point down.
Another certificate at this level grants read to this same group.
general access area for collaboration and "friends"
required_attribute group=group_a_admin enables (read and write and create_col) for http://ImgLib.gov/Lung_Collab/group_a with scope sub-tree
issuer= "Mary Thompson"
3
Mary Thompson delegates management of the group_a collection to anyone in group_a_admin.
Another certificate would define the access group as Lung_Collab only.
group_a
prototype group access area
(required_attribute CN="Mary Zolar" enables (read and write and create_col) and (required_attribute CN="John Walker" enables (read and write) for http://ImgLib.gov/Lung_Collab/group_a/data_a with scope sub-tree
issuer= "Jim Bean"
4
Jim Bean (in group_a_admin) delegates data_a collection management to investigator Mary Zolar and grants John Walker (Zolar co-worker) read and write (object create) permission.
prototype PI access area
data_a
data_b
data_c
Policy can be implemented by having the resource or its gateway structure relationships among groups.

Authorization Certificates for Apache

Akenti integrates with the unmodified Apache Web server by replacing the standard access control module ("htaccess").

Secure connection requests (https) pass the user identity certificate and the name of the requested resource to Akenti. Akenti then identifies all use-conditions, obtains the attribute certificates for the user, validates all certificates, and matches all use-conditions with attributes.

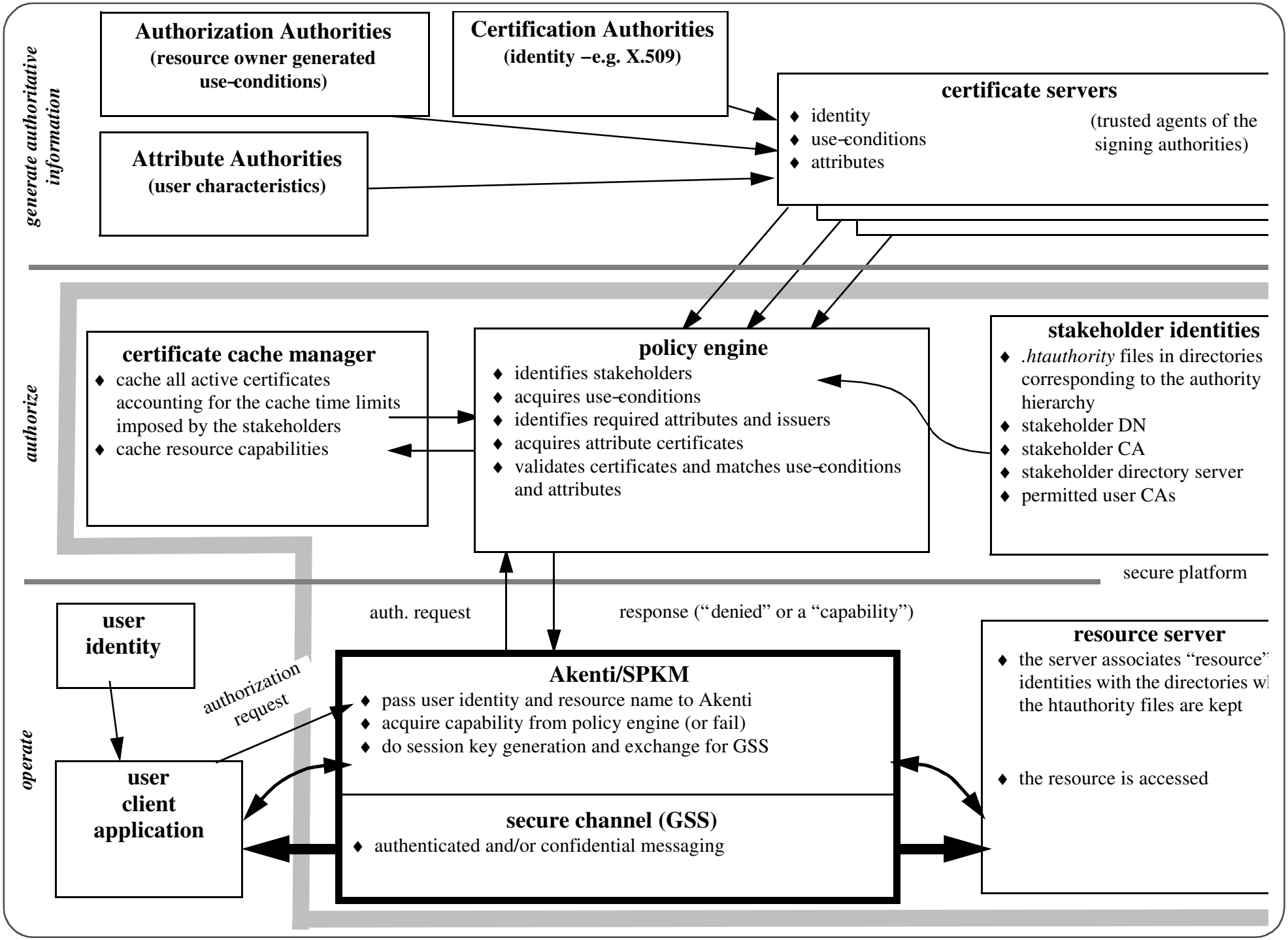

generate authoritative information
Authorization Authorities
(resource owner generated use-conditions)
Certification Authorities
(identity –e.g. X.509)
Attribute Authorities
(user characteristics)
certificate servers
identity
use-conditions
attributes
(trusted agents of the signing authorities)
authorize
certificate cache manager
cache all active certificates accounting for the cache time limits imposed by the stakeholders
cache resource capabilities
policy engine
identifies stakeholders
acquires use-conditions
identifies required attributes and issuers
acquires attribute certificates
validates certificates and matches use-conditions and attributes
stakeholder identities
.htauthority files in resource directories
stakeholder DN
stakeholder CA
stakeholder directory server
permitted user CAs
secure platform
user identity
auth. request
response ("denied" or a "capability")
authorization request
Apache
pass user identity and resource name to Akenti
acquire capability from policy engine
resource
fine-grained access control may be implemented by Web server resident methods that check for permitted actions
finally the resource –data-object or cgi-bin program –is accessed
operate
user client application
(e.g. Web browser)
secure channel (SSL)
set up security context between user-client and resource

Authorization Certificates for GSS-API

The integration of Akenti with GSS uses the Simple Public-Key Management protocol (SPKM). (SPKM is one of several standard protocols defined to do session key management for GSS.)

If the resource server has multiple functions, then these functions may be individually access controlled by imposing use-conditions on named "actions."

If a hierarchical authority policy model is required for multiple stakeholders, then *.htauthority* files can be placed in a directory hierarchy that is available to the resource server (actually to Akenti).


generate authoritative information
Authorization Authorities
(resource owner generated use-conditions)
Certification Authorities
(identity –e.g. X.509)
Attribute Authorities
(user characteristics)
certificate servers
identity
use-conditions
attributes
(trusted agents of the signing authorities)
authorize
certificate cache manager
cache all active certificates accounting for the cache time limits imposed by the stakeholders
cache resource capabilities
policy engine
identifies stakeholders
acquires use-conditions
identifies required attributes and issuers
acquires attribute certificates
validates certificates and matches use-conditions and attributes
stakeholder identities
.htauthority files in directories corresponding to the authority hierarchy
stakeholder DN
stakeholder CA
stakeholder directory server
permitted user CAs
secure platform
auth. request
response ("denied" or a "capability")
operate
user identity
authorization request
user client application
Akenti/SPKM
pass user identity and resource name to Akenti
acquire capability from policy engine (or fail)
do session key generation and exchange for GSS
secure channel (GSS)
authenticated and/or confidential messaging
resource server
the server associates "resource" identities with the directories wh the htauthority files are kept
the resource is accessed

Authorization Certificates for CORBA

Two approaches to integration of Akenti and CORBA:

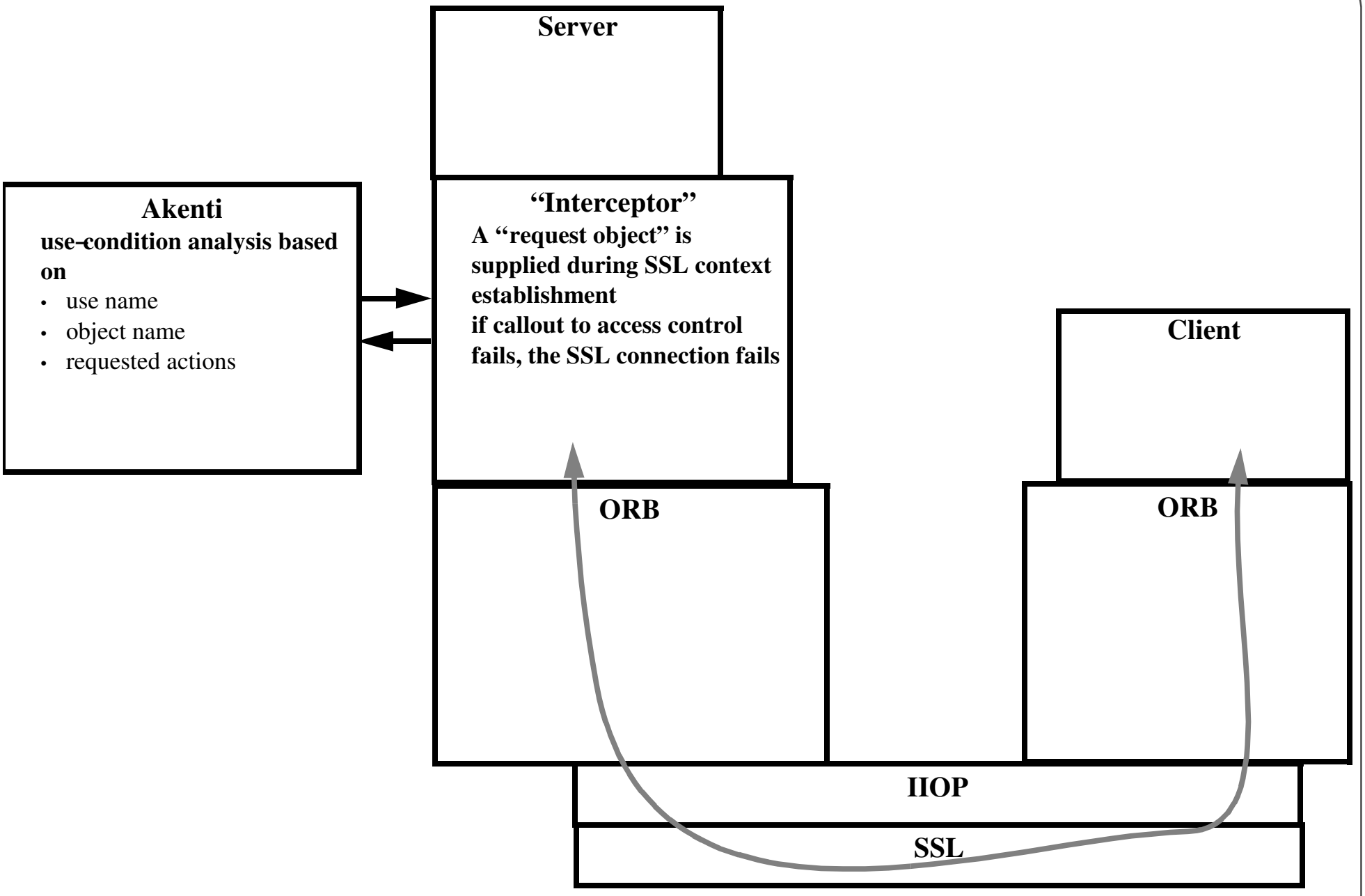
Use Akenti+SSL

- **coarse grained — only knows server identity, not functions**

Use OMG standard "intercepter" function to get

- **client certificate**
- **method being called**
- **OID**

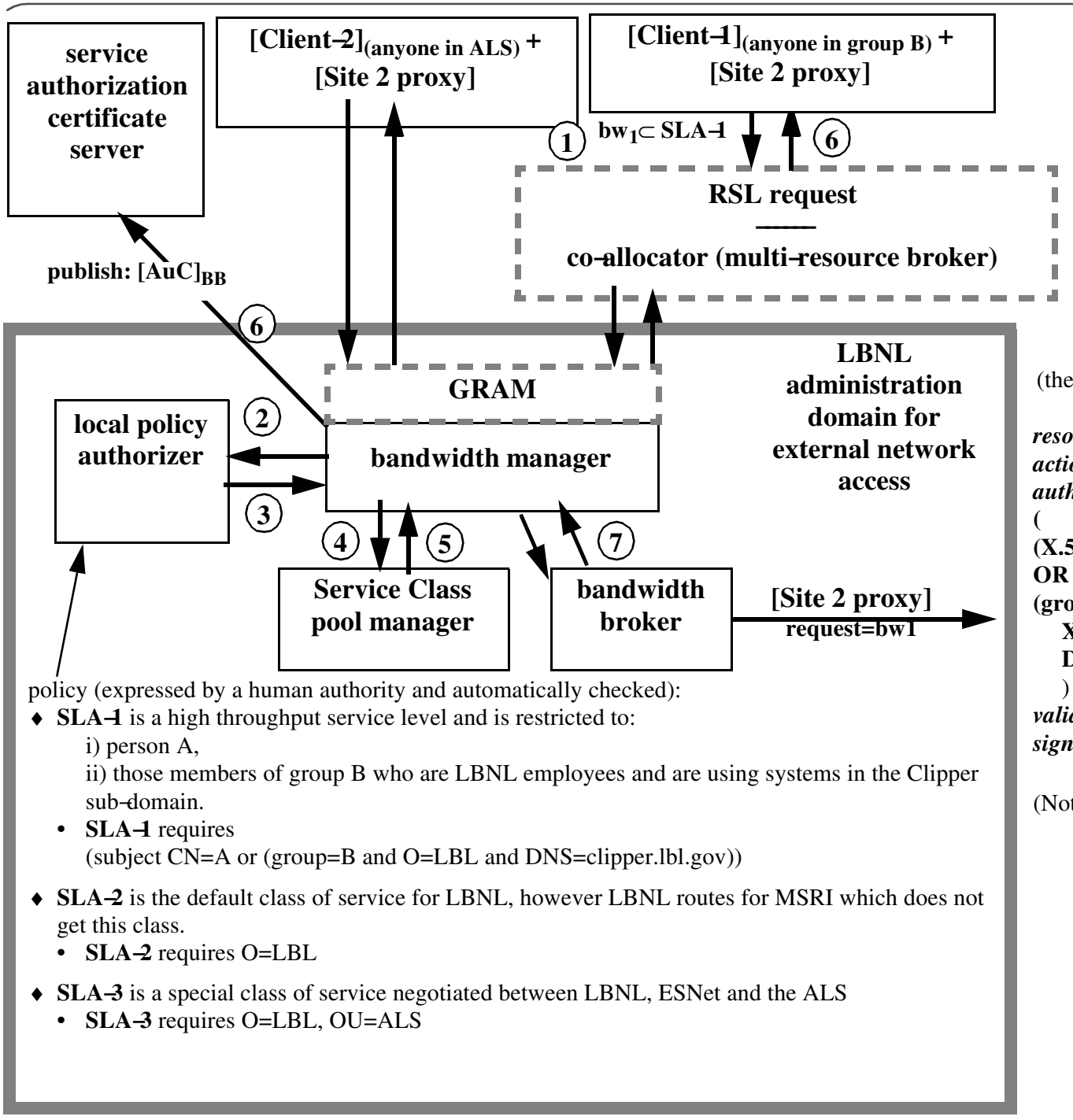
If the resource server has multiple functions, then these functions may be individually access controlled by imposing use-conditions on named methods and/or objects.



Akenti Integrated with A CORBA ORB using OMG "Interceptor" function

Bandwidth Reservation

Premium bandwidth request, policy-based authorization, and reservation phase (automated).



policy (expressed by a human authority and automatically checked):

- **SLA-1** is a high throughput service level and is restricted to:
  i) person A,
  ii) those members of group B who are LBNL employees and are using systems in the Clipper sub-domain.
  - **SLA-1** requires
    (subject CN=A or (group=B and O=LBL and DNS=clipper.lbl.gov))
- **SLA-2** is the default class of service for LBNL, however LBNL routes for MSRI which does not get this class.
  - **SLA-2** requires O=LBL
- **SLA-3** is a special class of service negotiated between LBNL, ESNet and the ALS
  - **SLA-3** requires O=LBL, OU=ALS

Authorization certificate ("AuC")
(the result of a policy-based decision to permit the use of this class of service)

resource **= SLA-1**
action **= 100 megabit/sec**
authorized **=**
(
(X.509@LBL-ca.lbl.gov:CN=A)
OR
(group=B@domain_A and
X.509@LBL-ca.lbl.gov:O=lbl.gov AND
DNS=clipper.lbl.gov)
)
validity times **= hour1:day1 –hour2:day2**
signed **= [message digest]BB**

(Note that "DNS=" is a runtime check.)

⇒ **Globus resource allocation mechanisms**