An Architectural Prototype for Certificate-based Authentication and Authorization

- **Sal Gurnani - University of California**
  - Project Scope
  - Design Considerations
  - University of California Certificate Authority and UC Directory

- **David Millman - Columbia University**
  - Columbia University Certificate Authority and CU Directory
  - Transaction Process
  - Open Issues
  - Next Steps
Project Scope

_tests an authentication protocol and operational model for using digital certificates for authentication
_tests a directory service to serve user attributes to determine the level of authorized access to licensed online materials
_does not address any issues involved in generating and distributing certificates by the institution.
Participants

- Digital Library Federation
- Columbia University
- University of California Office of the President
- JSTOR
- OCLC
Design Considerations - Localization of Information

- Must be able to allow the user to decide and convey if the transaction should be anonymous/stateless or unique/persistent.
- In a degraded condition where authorization is not available, an alternate level of service is provided.
- Only the institution (university, college, campus, etc.) can determine the affiliation and eligibility of each of its members to use each licensed publication, based on the license terms.
Design Considerations - Localization of Information

- Each eligible member will be assigned to (at least) one "class of service." The available classes are negotiated as part of the license agreement. For some publishers, there may be only a single class of service, for others there may be several.

- Only the publisher can determine the precise set of access permissions corresponding to a particular class of service, as specified in the license agreement with a particular institution.

- Allow for dynamic changes in user attributes. E.g., a person's status at an institution may change before the expiration date of their digital certificate from that institution.
Design Considerations - Privacy

- The institution should not be required to reveal information that can be used to identify a particular individual in order to allow that individual access to a licensed resource.

- Minimize the interface: only information strictly necessary to authenticate an individual and to authorize access should be exchanged as part of the transaction.

- Maximize reusability by minimizing the amount of institution-specific information that the publisher must keep, and the amount of publisher-specific information that the institution must keep.
Assumptions

- Each institution has its own certificate authority (CA) which is explicitly trusted by the publisher. Thus, the "Issuer" field in the certificate is sufficient to identify the institution.

- The institution must have a directory server which, given some information from the certificate, the publisher can query for user attributes and determine eligibility for the service.

- The full authentication and authorization process is performed infrequently (e.g., once per "session") so that minimizing the transaction cost is less critical.
University of California
Certificate Contents


**x509v3 Extensions (relevant subset)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetID*</td>
<td>Required</td>
<td>UC assigned unique ID for an individual</td>
</tr>
<tr>
<td>Strength Value*</td>
<td>Required</td>
<td>Certificate Issuance Identity Check Method/Strength for Individual</td>
</tr>
<tr>
<td>Campus Affiliation</td>
<td>Required</td>
<td>String value from set {OP, BK, DV, IR, LA, RV, SB, SC, SD, SF}</td>
</tr>
<tr>
<td>Auth. Pointer Type</td>
<td>Optional</td>
<td>String, ex. “URL”</td>
</tr>
</tbody>
</table>

* This field must be specified in order for the certificate to be a personal identity certificate. If the extension is not specified or missing, the certificate becomes an attribute certificate (see CPS).
University of California Directory Attributes

- **Affiliation**: optional, Faculty, staff, student
- **Campus**: optional, String value from set {OP, BK, DV, IR, LA, RV, SB, SC, SD, SF}
- **Serviceclass Object**
  - **Publisher**: required, String value defined by Publisher {jstor.org, oclc.org}
  - **Service**: required, String value defined by publisher {Null, FirstSearch}
  - **Class of Service**: required, String value defined by publisher {berkeley.edu, 100053231}
New Requirements

- OID 1.2.840.114006: CLIR

- OID 1.2.840.114006.1000: "Digital Library Authentication and Authorization Architecture"

- OID 1.2.840.114006.1000.1: query URL (this is the X509v3 extension)
Columbia University Certificate Contents

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 03:6f:7f:bc:38
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=US, ST=New York, L=New York City, O=Columbia University, OU=AcIS R&D, CN=AcIS Pilot Project CA
Validity
  Not Before: Mar 23 20:07:22 1999 GMT
  Not After : Oct 9 20:07:22 1999 GMT
Subject: C=US, ST=New York, L=New York City, O=Columbia University, OU=AcIS R&D Pilot Project, CN=5b5495da786f5977ff373d1ccf23341b
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
    {Key Data}
    Exponent: 65537 (0x10001)
X509v3 extensions:
  1.2.840.114006.1000.1:
daps://xsamd.cc.columbia.edu/ou=AcIS R&D Pilot Project,o=Columbia University,c=US?serviceClass?sub?(tempid=5b5495da786f5977ff373d1ccf23341b)
Signature Algorithm: md5WithRSAEncryption
    {Signature Data}
Columbia University Directory Content

* **dn:** other=922908404, ou=PilotPerson, ou=AcIS R&D Pilot Project, o=Columbia University, c=US
  other: 922908404
* **objectclass:** pilotPerson
  cn: HOLLY GOTHAM
  sn: GOTHAM
  uni: hbg27
  krbName: hbg27@CC.COLUMBIA.EDU
* **tempid:** 5467a891a6fba9dccc8286d140cfacf65
* **serviceclass:**::MCIECG9jbGMub3JnBAtGaXJzdFNIYXJjaAQJMTAwMDUzMjMx
* **serviceclass:**::MCAECWpzdG9yLm9yZwQFanN0b3IEDGNvbHVtYmlhLmVkdQ==
  description: acis pilot project data

⚠️ Only '*' fields are visible to publishers
⚠️ dn is "opaque"
⚠️ tempid is used for local certificate issuing method
⚠️ serviceclasses in this format are b64 encoded of asn1 der-encoding. decoded, they are:
  - serviceclass:: **oclc.org** FirstSearch 100053231
  - serviceclass:: **jstor.org** jstor columbia.edu
Transaction Protocol

- Publisher web server
- User/web-browser
- Certificates
- Institutional boundary
- Attribute/directory server
Transaction Protocol
Transaction Protocol

publisher web server

user/web-browser

attribute/directory server

institutional boundary

? valid certificate
? known institution
? location of institution’s attribute service
Transaction Protocol

publisher web server

? location of institution’s attribute service

attribute/directory server

user/web-browser

institutional boundary
Transaction Protocol
Transaction Protocol

1. publisher web server
2. user/web-browser
3. attribute/directory server

- ? valid publisher
- ? valid local user
- lookup user attributes in directory
Transaction Protocol

User/web-browser

Attribute/directory server

Publisher web server

Answer with appropriate user attributes for this publisher
Transaction Protocol

user attributes okay for service requested?
Transaction Protocol
Transaction Protocol Scales
Transaction Protocol Scales
Open Issues

- **Persistence of User Identity**
  - LDAP protocol always returns the distinguished name field
  - Methods for dissociating distinguished name from the user
  - Certificate Portability - mobile users, public workstation issues

- **Anonymous or “Attribute” Certificates**
  - Different certificate distribution possibilities
  - Not yet a stable standard

- **Hierarchical Certificate Authorities**
  - Certificate Authority chains of length > 1
Implementation Issues

- Attribute maintenance for each license
  - Individuals with multiple roles
- Directory service architecture and maintenance
  - Centralized vs. distributed directories (metadata directory with pointers)
- Attribute service unavailable - failover to a minimum level of service (contract specific)
Next Steps

- The architecture will need to be extended to handle the case in which the institution is not also the CA, possibly by requiring that the institution be identified in the "Subject" field.
- Expand the testbed to include three more educational institutions and three more publishers.
- Incorporate Transport Layer Security (TLS), in addition to Secure Socket Layer (SSL), as that standard becomes finalized.