An Architectural Prototype for Certificate-based Authentication and Authorization

Introduction

As an outgrowth of work from a Digital Library Federation (DLF) co- sponsored access management workshop and subsequent work by the DLF Architecture Committee, the current project aims to develop a digital certificate - based method for enabling access to licensed web- based information.

Scope

The DLF sponsored authentication project tests a protocol and operational model for using digital certificates for authentication and a directory service to serve user attributes to determine the level of authorized access to licensed online materials. It does not address any issues involved in generating and distributing certificates by the institution.

Design Considerations

Localization of information

- Must be able to allow the user to determine and convey the privacy and/or persistence associated with their user identity at the time of the transaction.
- 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 eligibility of each of its members to use each licensed publication, based on the license terms.
- 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 temporal change, e.g., a person's status at an institution may change before the expiration date of their digital certificate from that institution.

Privacy considerations

- The institution should not have 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 needs to 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

- In the case of institutions serving as their own CA, the institution is identifed in the "Issuer" field of the certificate.
- 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 the transaction cost need not be minimized.

Transaction Process

Following a user's attempt to access a particular service, and based on the assumption that the user has obtained a certificate from their institution, the following steps describe the transaction process:

- The user attempts to access the provider's web-based service at which time the user's certificate is sent
- The provider's server validates the certificate (issued by a known CA; not expired; valid signature; not revoked; other tests as deemed necessary)
- The query URL is extracted from the certificate and translated into an LDAP query

- The provider's LDAP client makes the LDAP query and captures the user's serviceClass information
- The serviceClass information is analyzed to determine whether the user should be given access to the service
- Access is then granted or denied based on the results of this analysis.

The result of the LDAP query may be kept in local cache with some reasonable expiry and referred to as needed. Subsequent contact with the provider's server will only require revalidation of the certificate.

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.
- Determine the ability of this model to support the delivery of use statistics specified by the International Consortium of Library Consortia in, "Guidelines for Statistical Measures of Usage of Web-based Resources," November 1998, http://www.library.yale.edu/consortia/webstats.html.