Systemwide Library and Scholarly Information Advisory Committee

Resolution C: Authentication of Authorized UC Library Users for Access to Digital Library Collections and Services

Resolved: ***The Systemwide Library and Scholarly Information Advisory Committee urges that reasonable technological means be taken to ensure that authorized UC students, faculty and staff are able to easily and reliably gain access to the digital information and services of the UC libraries from any location.***

- ***The Committee endorses the strategy being developed by the University to put in place a common, university-wide, robust and reliable digital credential system based on Public Key Infrastructure (PKI) as a long-run solution.***
- ***The Committee further strongly recommends that provision be made in the implementation of any digital credential system to preserve essential academic and intellectual freedoms by ensuring appropriate anonymity of individuals gaining access to on-line information. This requires that the University reveal to service providers only needed information about a certificate holder- e.g., that he/she is an eligible member of the University community under the terms and conditions of the contract with the provider.***
- ***Recognizing that full deployment of PKI technology throughout the University and the relevant industries will take at least three to five years, the Committee strongly advocates that campuses deploy and use proxy authentication servers as a cost-effective means to allow all faculty, staff and students access to digital library collections and services.***
- ***A universitywide digital credential system will support a wide variety of essential functions, and is therefore properly a campus and Universitywide responsibility. In view of the importance of this system for student and faculty access to library resources, the Committee strongly believes that library representatives must have a key role in planning and decision making for the system.***

Background: Authentication is the process a service uses to identify its users. Most commonly, this is accomplished by prompting a user for a login name and password. This has served well over the years, but as the number of services increases, people must maintain (and type) a growing number of login/password pairs. Another technique used extensively for digital library services is IP address; if a request is initiated from a campus network's IP address, it comes from someone physically located at that campus, and access to a service may be granted on that basis. This method does not work well, however, for the growing number of people who access the UC's digital library collections and services from non-campus locations.

Digital certificates deal with the issue of the rapidly growing number of services and the growing number of locations from which students, faculty and staff use those services. Digital certificates are becoming the World Wide Web's authentication method of choice. This means that, within a few years, we can expect most Internet sites to use digital certificates for authentication of individuals. Many commercial sites already do this, and

both the federal and state governments are moving in that direction, as well. This applies to library content providers as well, and the University has started including discussions of the use of digital certificates in license negotiations.

The UC Common Authentication Project has as its objective the establishment of a public-key infrastructure (PKI) with a common system-wide digital credential that will ensure that the University can comply with any access management controls that on-line information publishers may require. Authentication, in conjunction with University attribute servers, allows these services to establish the eligibility of the holder of the certificate. This identification may be:

- to a unique individual;
- to the anonymous group of all people who are issued certificates by the Certificate Authority, the University of California in this case;
- or to a semi-anonymous group, such as "undergraduates at UC Irvine."

Initially the use of digital certificates and attribute servers permit the University to reveal only the level of information about a certificate holder (e.g., that the holder is an undergraduate at UC, is an undergraduate at UC Irvine, etc.) that is required. The use of anonymous or semi-anonymous identification via the attribute server will be very important for library applications, as they will allow us to strike a balance between our need to provide anonymity to our patrons, while giving gross-level demographic information to content providers. In the future, special anonymous certificates may be used for the same purpose.

The use of PKI technology to establish eligibility for access to materials is relatively new and not yet widely or uniformly adopted in the industry. The University can play a leadership role in establishing practical and flexible protocols for the use of PKI credentials for this purpose. Such an outcome would benefit greatly not only the University but also the publishing industry generally.

However, it must be recognized that time and funding are needed to fully deploy the UC PKI throughout the University, and that additional time will be needed for full adoption of this technology by the publishing industry. While some technologically advanced publishers may be able to utilize UC's PKI in the near future, IP address authentication is the method commonly used by the libraries' vendors. Appropriately configured proxy servers at the campuses can be used as gateways to translate certificate-based authentication into IP-address-based authentication. For these reasons, the use of proxy servers, which have already been implemented by some campuses, will be necessary on an interim basis for a period of at least three to five years in order to provide authorized UC users at off-campus locations with simple and reliable access to the licensed digital content available through the UC library system.