ccess to on-line information resources and the use of electronic transactions increasingly augment the operation of modern colleges and universities. These resources and functions are important both internally and in collaboration with external partners. To reap the full benefits that these resources and processes can offer, all members of the campus community must be able to function easily and securely throughout this rapidly growing electronic information environment. Although campuses have made great strides toward developing robust and ubiquitous communications network infrastructures, the rich information environment envisioned in Sustaining Excellence in the 21st Century (Katz and West, 1992) will not be realized unless equally robust and ubiquitous enabling services are developed within the infrastructure of our campuses and throughout the higher education community.

I define the electronic information environment as that set of electronic information services, on-line resources, communications services, applications software, and workstations that enable us to teach and learn more effectively and without the constraints of time or place. Within this environment, we need directories and other finding aids, credentials that can establish identity and roles for both consumer and supplier, and a myriad of other supporting services. Infrastructure support services will enable easy and secure access to information resources, support authorized and verifiable transactions over the network, and make possible appropriate management of licensed materials and other intellectual property. With a coordinated approach, we will be able to leverage investments being made already in new applications on our campuses as well as across the higher education community.

As the electronic information environment grows and expands, it becomes necessary to acknowledge and implement certain constraints on users of these resources—the “network citizens” who navigate that environment. We must develop analogues of the administrative controls with which we are familiar in the traditional environment. These controls should be supported by generalized infrastructure services put in place and managed by the institution.

Existing access control and authentication mechanisms are largely a legacy of older centralized technologies. Traditional institutional applications have been developed from the ground up, providing for all aspects of the process in an idiosyncratic way. Today we understand that many of the components of these applications have a great deal of commonality. These include a secure and reliable way to affirm that users of our resources are who they purport to be and that they are authorized to use the resources to which they seek access. There must be a source of definitive information regarding their affiliation with the campus as well as other business-related data. There must be directory services to help them find the resources they need.

There must be standards and supporting services for encryption to secure data transmission and to create the digital equivalent of a personal signature. There must be efficient mechanisms to support accounting for the use of a wide variety of network-based resources as well as services that can be supported by network communications.

Lack of common general solutions for authentication, authorization, directory services, and encryption will impede the development of a broad range of information resources, from client-server financial systems to digital libraries. To properly designed, these technical building blocks can be combined and extended to form a set of common services, or “middleware,” that will enable a wide variety of complex capabilities that are available almost transparently to the end user (see Figure 1). These new and critical middleware services will enable members of the academic community to become true universal network citizens and roam freely and securely, without undue let or hindrance, throughout the emerging electronic information environment.

The availability and use of these and other building blocks also can form the basis for more robust and efficient management of institutional resources. Rule-based authorization processes can support distributed operation and...
The fundamental support service that will empower the network citizen is a universal, distributed, reliable, and robust digital credential system.

The firewall that has prevented many of the familiar problems and processes from finding their way to the campus is the physical distance between the campus and the external world. The electronic information environment is an increasingly complex territory in which valuable resources can be found, but it is foreign to our usual senses. The fundamental support service that will empower the network citizen is a universal, distributed, reliable, and robust digital credential system. Just as travelers must carry their passport when entering a different country, network citizens should carry a recognized credential when entering the electronic information environment. This credential, which can be validated by any service encountered, will ensure the authentic identity of the individual holding it.

Passports are recognized as authoritative around the world because the issuing authority is recognized by international treaty. So too should the network credential be recognized as authoritative so that network citizens can visit various sites and resources without having to resort to site-specific identification. Instead of an international treaty, there must be agreements among cooperating administrative domains to trust each other’s credentials. Such agreements are based on understanding the methodology and protocols that govern the process for issuing the credentials.

The concept of a digital credential that refers to a single entity is powerful because it can enable easy access to resources for the traveler. The credential itself may not contain much information about the individual, much as the traditional passport carries not much more than a picture, an address, and a passport number. But the travel credential can be used as a key to determining additional attributes about the holder. In an analogous way, the digital credential should have an identifier (e-ID) that is unique to the credential holder and can be used as a key to discovering further identity information.

Relying on a single credential is fraught with the potential for abuse if it is mishandled. Since e-IDs will let travelers into many places, they must be issued only with strong assurance that individuals are who they claim to be. Once the e-ID is issued, the holder must recognize that it is an extension of his or her personal identity, protect it carefully, and never lend it to another person.

Even with reliable credentials, it will be desirable in many cases for an individual to have several e-IDs to be used for different purposes. All individuals and their organizations must consider the potential impact of a compromise of the security of any e-ID. For example, the manager of an administrative computing system might have an e-ID that carries with it special privileges. That e-ID should be used sparingly and only in conjunction with that system so that compromise of the more powerful e-ID would have consequences of a more limited scope and could be dealt with more readily. The system manager would use a less powerful e-ID when doing routine work, such as checking e-mail or writing reports.

An e-ID represents an assertion on the part of a registration authority that a known individual or entity is represented by that e-ID. If the registration authority is well designed and reliable, then services in cooperating administrative domains, or realms, can be comfortable accepting those externally registered e-IDs. Thus, in the general case, the e-ID must indicate not only the registration authority that issued the e-ID. Ultimately this concept could be extended to commercial registration authorities so that, for example, someone can be the key to determining additional attributes about the holder. In an analogous way, the digital credential should have an identifier (e-ID) that is unique to the credential holder and can be used as a key to discovering further identity information.
Today we need generalized and scalable network-based mechanisms not only for authentication but also for eligibility and attribute information.
A digital signature must be some set of data that can not be forged and that binds the contents of a digital document to a specific individual, role, or other entity. It must be something that only the signing entity could have created and must be verifiable by anyone in the electronic information environment.

Standards now exist for creating this type of digital signature using public key cryptography (PKC). Clearly, digital signatures of this sort would enable a wide variety of institutional business to be transacted over the network with at least as reliable verification and auditability as we have now with paper forms and manual signatures.

A public key infrastructure (PKI) is crucial to enabling the use of encryption and digital signatures. Fundamental to the PKI is a unique pair of very large prime numbers, generated for each credential holder, that are keys used for encryption and decryption. This network software on the network citizen's workstation generates this pair of encryption keys and gives one of them (the "public" key) to the PKI certificate authority (CA). The other key (the "private" key) is closely guarded by the network citizen. The CA stores the public key in a directory along with the PKI certificate and its digital signature. The CA can then provide the public key to any application that requests it.

The basis for trusting a traditional signature is either direct knowledge or the ability to look it up in an archive maintained by a trusted authority, such as a bank. In the digital world, trust must be established through preestablished contracts based on mutual understanding of business practices, the basis for registering individuals with the CA, and the viability of the cooperating CAs.

A digital signature must be something that only the signing entity could have created and must be verifiable by anyone in the electronic information environment. This ability is part of an overall PKI and may be implemented in a number of different ways.

The basis for trusting a traditional signature is either direct knowledge or the ability to look it up in an archive maintained by a trusted authority, such as a bank. In the digital world, trust must be established through preestablished contracts based on mutual understanding of business practices, the basis for registering individuals with the CA, and the viability of the cooperating CAs.

The resulting so-called web of trust must be scalable to millions of users in thousands of locations. This can be achieved through a hierarchical model wherein a community-based CA registers subordinate CAs after verifying their viability. A consortium of college and university campuses, for example, could operate such a certificate authority and the associated services on behalf of its members. This CA in turn could register under national and international CAs to allow fully general and trustworthy access to verifiable public key directories servers anywhere in the world. A campus PKI with its root certificate authority also could register subordinate CAs for departments, the library, or special-purpose requirements.

Until and unless encryption mechanisms and support services are in use, no one should send anything of value or of a sensitive nature, such as a credit card number, over the data network.

A digital signature must be something that only the signing entity could have created and must be verifiable by anyone in the electronic information environment. This ability is part of an overall PKI and may be implemented in a number of different ways.

The basis for trusting a traditional signature is either direct knowledge or the ability to look it up in an archive maintained by a trusted authority, such as a bank. In the digital world, trust must be established through preestablished contracts based on mutual understanding of business practices, the basis for registering individuals with the CA, and the viability of the cooperating CAs.

The resulting so-called web of trust must be scalable to millions of users in thousands of locations. This can be achieved through a hierarchical model wherein a community-based CA registers subordinate CAs after verifying their viability. A consortium of college and university campuses, for example, could operate such a certificate authority and the associated services on behalf of its members. This CA in turn could register under national and international CAs to allow fully general and trustworthy access to verifiable public key directories servers anywhere in the world. A campus PKI with its root certificate authority also could register subordinate CAs for departments, the library, or special-purpose requirements.

Until and unless encryption mechanisms and support services are in use, no one should send anything of value or of a sensitive nature, such as a credit card number, over the data network.
each campus that can include a wide variety of information, including affiliation and eligibility data.

- Directory and resource location servers
- PKI servers that manage certificates and public encryption keys for individual users and make possible digital signature verification
- Electronic license servers in support of site-licensed software, library materials, and databases
- Billing transaction servers that can handle a large volume of small-value debit records extremely efficiently
- Time servers and digital notary servers that form the basis for reliable and verifiable on-line content and digital institutional archives

Figure 2 shows how the building blocks might relate to each other and to the communications system and applications programs. Other building blocks might include software version control servers to ensure that campus users have access to the latest version of critical application programs, and alias servers to support consistent mapping between e-IDs and e-mail addresses or traditional identifiers such as employee number or student ID number. Current and potential technologies behind each of the building blocks described above are in different states of development and deployment.

With persistent vision and cooperative efforts, we can refine and deploy appropriate versions of all these enabling services over the next few years. If we do not start now, it may become very difficult to develop and retrofit a coordinated set of these services later. There is much to be done before network citizens are fully empowered.

Note
M. Stuart Lynn, a colleague and friend to most of us in the information technology community, provided ideas, advice, counsel, and encouragement in the creation of this chapter.

Reference

The “E” Is for Everything is the second volume in the EDUCAUSE Leadership Strategies series, sponsored by PricewaterhouseCoopers. A complimentary copy of the book has been sent to the primary representative at each EDUCAUSE member institution and organization; additional copies may be purchased from Jossey-Bass (see http://www.josseybass.com) or from EDUCAUSE (see http://www.educause.edu/pub/pubs.html#books).

END USERS AND APPLICATIONS SOFTWARE

Network Accounting and Billing Services
Licenses Server
Resource Location Servers
Network Time Server
Authentication Server
Public Key Infrastructure Certification Authority
Attribute and Eligibility Servers
Network Communications Infrastructure

Figure 2. Information Environment Building Blocks with Common Interoperable Solutions for Basic Supporting Services

EDUCAUSE Strategic Initiatives Fund

A small group of corporate friends provides undesignated funding to support EDUCAUSE explorations in new areas of strategic importance. These gifts make it possible for EDUCAUSE to remain on the leading edge in matters of utmost importance to higher education.

Companies that have contributed to this fund in the year 2000 include:

- Datatel, Inc.
- Dell Computer Corporation
- IBM Corporation
- SCT
- WebCT

EDUCAUSE and its higher education members appreciate the support of its corporate community. We will continue to build unique and meaningful forums to bring corporate leaders together with their colleagues and customers in higher education.

For more information:
corp@educause.edu
www.educause.edu/partners

EDUCAUSE and its higher education members appreciate the support of its corporate community. We will continue to build unique and meaningful forums to bring corporate leaders together with their colleagues and customers in higher education.

For more information:
corp@educause.edu
www.educause.edu/partners

EDUCAUSE 2000

Join us October 10–13, 2000 for higher education’s premier IT conference at the fabulous Opryland Hotel in Nashville

- Featured speakers: Dave Barry, David Habersatt, Judy Estrin
- 150 Track sessions
- 30 Preconference Seminars
- 150 Corporate Exhibits
- Workshops, presentations, poster sessions, current issues sessions, constituent groups
- A Thursday evening roundup at the Wild Horse Saloon, featuring the Nitty Gritty Dirt Band

Don’t wait! Reserve your room at the Opryland Hotel now!

Visit the conference Web site www.educause.edu/conferences2000 and register today.