

## PKI technologies

### Evolving Technologies Committee 2000

PKI (public key infrastructure) includes a substantial suite of technologies and services that are rapidly evolving to enable campus networks and the Internet to meet the “legal”, “business”, “privacy”, and “intellectual property” requirements of higher education in addition to proving access and connections.

A complete PKI system enables capabilities commonly referred to as authentication, authorization, access control, confidentiality, data integrity, and technical non-repudiation. Together, these capabilities go far toward making the network a “safe” and “reliable” place in the business, legal, and policy sense.

Although the basic components and methods of PKI have been known for some time and have been deployed in special circumstances, they are just now “emerging” in the sense of widespread deployment in higher education as well as business. They do not directly extend or replace previous network technologies (such as logins and passwords), but instead bring the full range of capabilities that we enjoy in the world of paper to the network.

The capabilities enabled by PKI are truly essential if higher education is ever to move its core means of access and communications to the network. These capabilities are every bit as important for learning and research as for administration. They all come together in the requirements for Internet-based distance learning.

Another reason they will enter the mainstream is that our partners and providers such as publishers, libraries, other content providers, support services, financial institutions, federal agencies, etc., are all rapidly adopting the new “Internet” mode of access and communications. They are driving the deployment of PKI into commercial products and services that higher education simply must use.

PKI is now at a level of very high interest in higher education. A small number of campuses are moving down the path toward a comprehensive plan and solution. Others are studying their options and learning the basics. Most are just becoming aware of the issues involved. The pressure to adopt solutions soon is mounting rapidly, however, so that we may expect to see a much deeper and broader effort in the next years

Although the concepts of PKI are not especially new, they are only now moving into commercial products and services in a large way (e.g., in Windows 2000) due to the rapid evolution of the commercial Internet. Although some products lag others and there are technical issues of direction and compatibility, the real issue for higher education is one of standardization and interoperability. Campuses must choose solutions from a large number of options that will not only work across the various units of the campus, but that will interoperate with other campuses, federal agencies, and commercial partners. This is especially tricky because the standards for PKI are not specified to the level of detail that determines how to do this. (How many characters in what form are used to specify a student’s name? What does the term student mean on your campus, anyway?)

The real evolution is one of large-scale re-engineering of campus functions. The network has the capability of bringing the hundreds of databases, identification checks, security codes, and silo services that we use today together into a common framework, but at the eventual cost of changing most of the associated human systems and policies.

a.) Research

Research, even “pure” academic research, is very much dependent on the capabilities of PKI to guarantee secure access and communications until time for “free and open” publication. Large-scale Research cannot fully move to the Internet until these and related business capabilities are in place.

b.) Teaching

Proper, controlled access and identification are critical to our systems of learning, teaching, and academic management. Our business functions involve all students, faculty, staff, partners, suppliers, financial institutions, agencies, etc. Traditional methods used on campus simply will not work through today’s network. PKI is absolutely essential if this is all to come together to support Internet-based distance learning.

c.) Production Management

PKI will be used to enable most aspects of remote management, whether of devices or of people.

d.) TCO

TCO of PKI is difficult to estimate. It will be quite expensive to implement full-scale PKI systems even though much of the software is “free.” Other costs include professional management of directories, protection from legal liabilities, possible fees for “certificates”, and, most importantly, the very large cost in time and dollars of re-engineering the operations of a campus.

The payback of a successful system is also very large, however, leading to a significant rush in the commercial world to undergo the transformation to an “e-company” in business-to-business if not business-to-customer communications. There is no reason to believe that similar economics will not apply for higher education.

A rating might be determined by the breadth/depth of impact on the full range of university business.

PKI enables remote access by students and faculty to nearly every function of a campus, supports the business-to-business communications of the campus with partners, suppliers, the federal government, banks, and others, and eventually requires a re-engineering of many operations in all walks of campus business.