

## Digital Certificates: Coming of Age

**D**igital certificates are part of a developing set of technologies that can address many of today's security, identity, and accessibility issues. Acting as a kind of digital ID card, digital certificates are issued to Web servers or individuals. Anyone using a popular Web browser to surf the Web has a cache of perhaps sixty pre-installed digital certificates that the browser relies on for secure access to Web sites—without the user's awareness or intervention.

The use of these security technologies has been quietly growing and maturing. Digital certificates are the core of a public key infrastructure (PKI). Commercial companies such as VeriSign and non-profits such as CREN, the Corporation for Research and Educational Networking—a member organization of over two hundred universities, colleges, and research organizations (<http://www.cren.net>)—play a key role as certificate authorities, issuing and managing institutional certificates, Web server certificates, and end-user certificates. States, such as Illinois, have acquired certificate services for their citizens, anticipating that much business, from signing contracts to reserving cabins in parks, will be carried out over the Internet and will need, in many cases, to be legally binding. The Electronic Signatures in Global and National Commerce Act of 2000 creates the legal framework for this dramatic change.

Where does the academic community fit in? It is time to consider both the potential value and the potential risks of these technologies for colleges and universities and to address the policies for the use of digital certificates on campus.

Although the use of certificates to exchange secure information between Web browsers and servers is perhaps the most widely deployed use of digital certificates on campus, other uses will be just as significant and less transparent. Students, faculty, and staff will soon be using certificates for authenticating themselves to Web services and resources and for signing and encrypting e-mail. On some campuses, this is already happening. In the future, as institutions learn how to effectively provide quality of service over computer networks, faculty may use certificates to guarantee bandwidth for a class or similar priority activities.

More immediately, certificates are ideal for students and faculty who need to update or access personal information such as addresses and private information such as grades. Federal agencies, including the Department of Education and the Immigration and Naturalization Service, are looking closely at digital certificate services as a way for agencies, colleges/universities, and students to collectively participate in providing up-to-date, verifiable information. One reason many higher education institutions are seriously exploring certificate services is the expectation that the federal government will require certificate use in the next two years. A key effort enabling end-to-end trust paths for interinstitutional use of PKI is the EDUCAUSE work on a Higher Education Bridge Certification Authority (HEBCA).<sup>1</sup>

A frequently asked question is how soon these digital certificate services will be required on campuses. PKI has been “two years out” for over five years, but much progress is being made. Still, the lack of important user-friendly client

components has created unfortunate and annoying barriers. For example, it is relatively easy for users to download campus-based and institutional-based root certificates. But downloading root certificates is an extra step requiring users to be aware of the need for a root certificate to match the issuer of their certificates. With the release of the new Opera Software browser containing the CREN roots, users will not need to be aware of this requirement while using the Opera browser.

Is there a killer application that will drive the development of an unobtrusive, easy-to-use PKI infrastructure? So far, there are many promising applications, including secure e-mail and secure administrative services such as document signing. Though perhaps not (yet) a killer app, secure e-mail is a likely candidate. As more and more users have digital certificates, users will routinely encrypt and decrypt and verify their mail. Yet a search for a digital certificate killer app may not be important, since PKI is “beginning to morph into a set of security functions embedded in applications, operating systems, and product offerings that combine authentication and access control.”<sup>2</sup>

Another valuable use of digital certificates is for sharing information among trusted partner institutions and communities. For example, the University of Illinois and Cornell University might agree to share the materials from a set of cooperative courses. Rather than each school having to validate student identities from both institutions, each institution can agree to trust certificates issued by the other. In simple terms, Cornell can say, “If Illinois states that Jane Doe is a student of theirs, then we'll trust requests for services from

Jane Doe." This is accomplished by creating trust relationships between the services at each school and by relying on digital certificates. Each institution can be confident of the validity of the other's certificates because each has a trust relationship with a "root" authority like CREN. (With the recent closing of CREN, these institutional certificate services are now being managed by Internet2.) The signature of the CREN root authority on an institution's certificates provides assurance that the certificates have been issued by that institution. In fact, the creation of higher education certificate authorities is a critical step in building interoperable services that will help colleges and universities realize the promise of nationally or globally shared resources while respecting intellectual property, licensing, and other constraints on sharing.

Understanding the uses of digital certificates is not enough; higher education institutions need tools for issuing digital certificates to their communities. Some tools, such as the open-source Papyrus software from Georgia Tech, enable colleges and universities to build an extensible certificate system easily and cost-effectively. The philosophy of Papyrus is simple. Because every institution's needs and processes are likely to be unique, Papyrus provides a flexible toolkit and cryptographic library for setting up campus certificate services.<sup>3</sup>

Dartmouth College, with support from the Andrew W. Mellon Foundation, is working with other institutions to facilitate the use of digital certificates on campuses. In their current form, PKI deployments are still too complex, costly, and time-consuming for most campuses. The Dartmouth PKI lab (<http://www.dartmouth.edu/~pkilab/>) is thus working to develop and disseminate knowledge and tools that lower the barriers to using PKI technologies. Reports on digital certificate products and software toolkits, field-tested user documentation, sample application code, and application enhancements are all being developed at the lab.

In addition, applications requiring authentication and authorization are being modified to use certificates, and new applications not possible without PKI are being tested in the real-world, controllable microcosm of Dartmouth. Universal

availability is a critical factor for many of the more compelling applications of PKI. For example, secure e-mail obviously requires both sender and receiver to be compatibly equipped. Once users can assume that their secure messages will be received, both usage and new applications should increase.

Existing PKI-enhanced applications often have serious security flaws. For example, electronic documents with active content features can be relatively easily manipulated so that their displays are changed in usefully malicious ways while not invalidating the PKI signature on the document. Virtually all elements of the Web browser display, including the SSL lock icon and the server certificate window, can be replaced by a malicious Web site. Dartmouth is investigating security flaws in current software products. The results of these studies are being published to hasten the development of improved products. For the latter case, students in the Dartmouth PKI lab have developed Web browser modifications to solve the problem.

CREN, as part of a Mellon Foundation Planning Grant, had been working to demonstrate certificate-based authentication and authorization for access to Web publishers' sites. The WAVE1 group successfully demonstrated such interactions with the JSTOR system. PKI is an attractive alternative to account/password or IP-based access control.<sup>4</sup>

Another important development in the authorization space is the Shibboleth project, created by Internet2 and its partners to develop an open, standards-based solution for organizations to exchange information about their users in a secure and privacy-preserving manner. The system preserves the privacy of individuals by using class identity, rather than an individual's identity, as the default authorization and by allowing users to determine whether to release additional information about themselves.

What about the policy issues? Policy is as important a component in an operational PKI as is the cryptography. Much of the work on higher education campuses is currently built on PKI-Lite—that is, full-featured PKI technology deployed with existing campus standards for identification and authentication (I&A) and

security. The PKI-Lite trust environment was developed by the Higher Education PKI Technical Activities Group (HEPKI-TAG) and the Higher Education PKI Policy Activities Group (HEPKI-PAG) to promote the use of digital certificates on campuses by matching the majority of campus application needs to the corresponding security and risk requirements.

In conclusion, the basic technologies for PKI are being built and deployed at leading higher education institutions and academic consortia, as well as in industry. The legislative enablers are in place, as are the basic components of the federal infrastructure and higher education certificate authorities. At the same time, there is a critical need within the community—a need for secure communications, trusted services, and reliable authentication and authorization for access to those services, both within the campus and with outside agencies and other colleges and universities. The looming requirements at the state and federal levels may be motivation enough for institutional leaders to begin serious investment in certificate-based services, but the greatest value of investing in this technology lies in the kinds of services that a campus can build for its own community. Certificates are quietly coming of age.

#### Notes

1. See Mark A. Luker, "A Bridge for Trusted Electronic Communications in Higher Education and the Federal Government," *EDUCAUSE Review* 37, no. 1 (January/February 2002): 40-49 <<http://www.educause.edu/ir/library/pdf/erm0203.pdf>> (accessed October 28, 2002).
2. Vic Wheatman, "PKI: What Is It Good For?" *Gartner Top View Report*, AV-14-1092 (July 26, 2001), 5.
3. For more on the Papyrus project, see <<http://www.cren.net/crenca/crencapages/papyrus.html>>.
4. For more on the WAVE1 project, see <<http://www.cren.net/crenca/cproject/wave1/index.html>>.

**Judith V. Boettcher is the Executive Director of CREN and a frequent author and presenter. Robert Brentrup, Associate Director for Technical Services at Dartmouth College, is co-Principal Investigator of the PKI Lab. John Douglass, with the Georgia Institute of Technology, is the developer of Papyrus, an open-source-based certificate authority system.**

