Digital Certificates

What Are They, and What Are They Doing in My Browser?

By Judith V. Boettcher and Amanda Powell

Digital certificates provide a means to authenticate individuals and secure communications on campus. CREN now offers an easy way for institutions to learn about and deploy this powerful technology.

Did you know that you have a cache of digital certificates in your Web browser? In fact, you probably have more than 60 digital certificates that come preinstalled in the Netscape and Internet Explorer browsers. These certificates are from vendors such as VeriSign, Entrust, and Baltimore. Your Web browser uses them for secure access to Web sites—without your even being aware of the presence of the certificates.

What are Digital Certificates?

Digital Certificates are part of a technology called Public Key Infrastructure or PKI. Digital certificates have been described as virtual ID cards. This is a useful analogy. There are many ways that digital certificates and ID cards really are the same. Both ID cards and client digital certificates contain information about you, such as your name, and information about the organization that issued the certificate or card to you.

Universities generally issue institutional ID cards only after ensuring or validating that you are a bona fide student, faculty, or staff member. In PKI terms, this is called the *registration process*—verifying that you are eligible to receive a certificate and verifying the information in it.

Similar to an important ID card, once a digital certificate is issued, it should be managed with care. Just as you would not lend someone else your ID card allowing entry into a secure facility, you should never lend someone your digital certificate. If your certificate or ID card is lost or stolen, it should be reported to the issuing office so that it can be invalidated and a new one issued.

How is a digital certificate created? In creating digital certificates a unique cryptographic key pair is generated. One of these keys is referred to as a public key and the other as a private key. Then the certification authority—generally on your campus—creates a digital certificate by combining information about you and the issuing organization with the public key and digitally signing the whole thing. This is very much like an organization's ID office filling out an ID card for you and then signing it to make it official.

In PKI terms, the public key for an individual is put into a digital document, along with information about that individual, and then the digital document is signed by the organization's certification authority. This signed document can be transmitted to anyone and used to identify the subject of the certificate. However, the private key of the original key pair must be securely managed and never given to anyone else. As the private key is a very large prime number, it is not something an individual memorizes; rather, the private key must be stored on some device, such as a laptop computer, PDA, or USB key ring.

If you send a copy of your certificate to another computer to authenticate yourself, what keeps someone with access to that computer from reusing it later to pretend to be you? Unlike an ID card which is valuable by itself, the digital certificate is useless without the associated private key. That is why protecting the private key is so important. The private key must never be given to anyone else nor left somewhere outside of control by the owner.

An added value of digital certificates is that they provide a higher level of security than what we currently have with PIN and password combinations. Users still use passwords, but only on their local computer to protect their digital certificates. If one loses the device on which a digital certificate is stored, a person holding the certificate would still need the password to unlock the certificate.

What is a Digital Signature?

Above we stated that the digital certificate was digitally signed. The holder of a digital certificate can also use it to digitally sign other digital documents, for example, purchase orders, grant applications, financial reports or student transcripts. A digital signature is not an image of your pen and ink signature—it is an attachment to a document that contains an encrypted version of the document created using the signer's private key.

Once a document is signed, no part of that document can be changed without invalidating the signature. Thus if someone obtained a copy of your digital certificate and changed the name in it to be their own name, any application receiving that modified certificate would see immediately that the signature on it was not valid. In this sense, a digital credential is much better than a traditional ID card to prove that the holder is really the person to whom it was issued. In fact, digital signatures in general are much more useful than pen and ink signatures since anyone checking the signature also can find out something about the signer in order to know whether the signature is meaningful.

Public Key Infrastructures and Certificate Authorities

Digital certificates are one part of a set of components that make up a public key infrastructure (PKI). A PKI includes organizations called *certification authorities* (CAs) that issue, manage, and revoke digital certificates; organizations called

relying parties who use the certificates as indicators of authentication, and clients who request, manage, and use certificates. A CA might create a separate *registration authority* (RA) to handle the task of identifying individuals who apply for certificates. Examples of certification authorities include VeriSign, a well-known commercial provider, and the CREN Certificate Authority that is available for higher education institutions.

In addition to the organizational roles, there must be an associated database or directory, generally using a directory access protocol called LDAP, that will store information about certificate holders and their certificates. There also must be a way to make available information about revoked certificates. An application that makes use of PKI digital credentials may consult the revocation database before relying on the validity of a certificate. It may wish to consult the Subject directory as well in order to retrieve further information about the certificate Subject.

Types of Certificates

There are different types of certificates, each with different functions and this can be confusing. It helps to differentiate between at least four types of certificates. You can see samples of some of these different types of certificates in your browser.

- **Root or authority certificates.** These are certificates that create the base (or root) of a certification authority hierarchy, such as Thawte or CREN. These certificates are not signed by another CA—they are *self signed* by the CA that created them. When a certificate is self-signed, it means that the name in the Issuer field is the same as the name in the Subject Field.
- **Institutional authority certificates.** These certificates are also called *campus certificates*. These certificates are signed by a third party verifying

the authenticity of a campus certification authority. Campuses then use their "authority" to issue client certificates for faculty, staff, and students.

- **Client certificates.** These are also known as end-entity certificates, identity certificates, or personal certificates. The Issuer is typically the campus CA.
- **Web server certificates.** These certificates are used to secure communications to and from Web servers, for example when you buy something on the Web. They are called *server-side certificates.* The Subject name in a server certificate is the DNS name of the server.

Getting Hands-On with Certificates

To see the certificates in your browser, including some you may have unwittingly installed yourself, you can go to the Preferences menu in Netscape/Windows, and from the Privacy and Security Menu, select the Certificates option. From this option, you can manage the Authorities certificates that come preinstalled in your browser and also manage your personal certificates. You can view, edit privileges, or even delete certificates.

You can also view and manage certificates within Internet Explorer/Windows by selecting Internet Options from the Tools menu and then choosing Content. Then, by selecting Certificates, you can manage your Trusted Root Certificates as well as your personal certificates. In Netscape/Mac, just select the Security icon.

Digital Certificates in Higher Education

Digital certificates and the PKI infrastructure are a broad-enabling technology. This means that once the technology is deployed, it is planned to be widely adopted and used by many different applications. Instituting the use of digital

certificates on campus for faculty, staff, and students generally is done at the central IT level. However, adopting this technology should have support from the highest levels of the campus administration since it may become critical to a large part of the operation of the campus.

Some of the campuses that are deploying digital certificates include Columbia, MIT, and the University of Texas-Houston. Other institutions that are planning for deployment include the University of Minnesota, Dartmouth, Georgia Tech, and the University of California system. Some campuses are operating their own PKI technology while others are out-sourcing all or part of it.

The broadest use of digital certificates on campuses is the use of web server certificates. These certificates enable the encryption of communications to and from webservers to protect sensitive personal information such as credit card and other financial or health information.

Individuals use digital certificates for two main purposes: (1) to authenticate themselves to a Web service or to a network resource and (2) to sign and, if desired, to encrypt documents such as e-mail. For example, higher education institutions are designing campus systems to use digital certificates for authenticating individuals for Web services such as updating personal information files; for viewing grades and financial status; for course registrations, residence lotteries, - business services, and voting; and for remote access to resources, such as licensed on-line information, class material or health services. Electronic mail for general business use as well as for the submission of timesheets, travel reports, and service orders is another application which can benefit greatly by the use of PKI.

Digital certificate technologies also can support the desire on many campuses to create single sign-on authentication and authorization systems that reduce the need for many sign-ons and password combinations that are inevitably hard to manage. With just a little experience, users can easily manage their digital certificates within their browser or with other applications.

Getting Started with Digital Certificates

To set up a Certification Authority on campus, an institution needs to acquire hardware and software for the two primary functions of registering individuals and issuing certificates. Campuses must also have or develop an campus-wide directory to provide information about certificate holders, and determine the organizational and policy framework for their certification authority. The policy framework is similar to existing policies on campuses as to who receives a campus identification card. The policy defines who in eligible to get a certificate, how identification of Subjects is done and by whom, how the hardware and software components are managed, and how certificates are managed over their lifetime.

There are commercial vendors of PKI services. Typically these vendors will charge a modest annual fee per certificate or per certificate subject. The institution contracting for these services still must be responsible for identifying eligible certificate holders, managing the associated campus-wide directory, and managing the certificate renewal and revocation processes.

In addition to the basic PKI components, certificate users will need browsers that can cache and make use of PKI certificates, and may require some help desk assistance in using them. Applications that want to make use of certificates issued by the institution will need to be modified to recognize them and will need a copy of the authority certificate for the CA.

PKI-Lite lowers the barriers to getting started

PKI and digital certificates can easily bring improved security to campus communications and services. However, the PKI trust environment for financial purposes and some federal government applications has made standard PKI costly and complex to deploy. As you can tell from the descriptions above, a full PKI implementation involves a great deal of time and expense. Recognizing this, the higher education technical community has developed a "PKI-Lite" trust environment designed to lower the barriers for the deployment of digital certificates on campuses. The PKI-Lite trust environment is intended to promote the use of digital certificates on campuses by matching the majority of campus application needs to the corresponding security and risk requirements.

PKI-Lite 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). The PKI-Lite environment depends on the following three trust documents:

- A combination Certificate Policy and Certificate Practice Statement. This combined CP/CPS describes the recommended best practices for a campus certificate authority to use for the PKI-Lite environment.
- A recommended profile for the x.509 v3 PKI-Lite certificates.
- A relying party statement for organizations that will rely on the authenticity of certificates issued in the PKI-Lite trust environment.

The documents listed above are available at http://www.cren.net/crenca/pkiresources/index.html. Also on that page is a

link to the Guide to Getting Started With Digital Certificates as well as a number of other useful PKI and digital certificate knowledge resources.

The CREN Digital Certificate Services

CREN currently offers an expanded set of certificate authority services to higher education institutions.

- CREN-signed campus certificates for institutions. These CREN-signed certificates are for institutions issuing certificates for their campus community—in the range of 10 or more Web server certificates and for more than 500-1000 client certificates.
- CREN Web server certificates. These certificates are for campuses to use for securing Web servers, supporting a range of campus Web applications.
- Client certificates. CREN has an internal CREN.NET service equivalent to a campus certificate-issuing application. A registration contact at a campus validates/approves individuals and CREN issues the certificates. These certificates can be used to communicate with vendors, agencies, and so on.

With these three levels of service — including the free test certificates — CREN can help campuses get started using digital certificates at a level matching their particular campus needs.

More detailed descriptions of each of these CREN CA Digital Certificate Services, along with an opportunity to try out a digital certificate, can be found at: http://www.cren.net/crenca.

Test Drive a Digital Certificate: The CREN Test CA Demonstration Site

Understanding new technologies is always easier when you have personal experience with a technology. The CREN Test Demonstration site is a place for members of the higher education community to experience how digital certificates work. The site issues personal client digital certificates for use in testing, piloting, and educational uses.

Just go to http://www.cren.net/crenca/ctca/ select "CREN Test CA"—the wizard will walk you through the steps for obtaining your CREN-signed personal certificate and loading it into your browser. When you've picked up the certificate, you can play the classic game of asteroids to see how you use your certificate for access to web resources. When you're finished, please remember to leave feedback by using your certificate to access the online questionnaire. If you have any difficulty, simply e-mail digicert@cren.net.

The CREN Test CA Demonstration site was a collaborative project of John Douglass of Georgia Tech and Michelle Gildea, Arya Parsee, and Jim Reynolds of CREN.

Judith Boettcher is the executive director of CREN and can be reached at jboettch@cren.net. Amanda Powell is the membership communications manager at CREN and can be e-mailed at apowell@cren.net. David Wasley is leading the PKI planning at the University of California Office of the President.