Digital Certificate Infrastructure

Frequently Asked Questions

Providing secure, low cost, and easy access to distributed instructional and research resources is a growing problem for campus library and information technology professionals. This FAQ provides information on the use of digital certificates as a means of authentication for distributed access to resources. It is designed for two audiences: university librarians and staff responsible for licensed content contracts, and university administrators—presidents, provosts, and directors of campus information technology.

Published by the Digital Library Federation (DLF) and the Corporation for Research and Educational Networking (CREN)

Section One:
Introduction to Digital Certificates

1. Why are digital certificates important for libraries and campuses?

- There is a national movement to use digital certificates to authenticate and authorize secure interactions over the network.
- Digital certificates provide a single method of authentication and access control for all internal, academic, and administrative applications.
- Digital certificates provide a single method of authentication and access control for remote faculty and staff and for remote applications, including applications being developed for Internet2.
- Digital certificates provide a mechanism to integrate and consolidate a wide variety of disparate access management systems into a single, standards-based system.
- Digital certificates are easy to use and are already supported by all Web browsers.
- Digital certificates provide encryption capability.
- The public-private keys used with digital certificates can be used to develop digital signature services for administrative applications and electronic mail.

2. What are digital certificates? What do they do?

Digital certificates are digital files that certify the identity of an individual or institution seeking access to computer-based information. In enabling such access, they serve the same purpose as a driver's license or library card. The digital certificate links the identifier of an individual or institution to a digital *public key*.

3. What is a digital "public key"?

The combination of standards, protocols, and software that support digital certificates is called a *public key infrastructure*, or PKI. The software that supports this infrastructure generates sets of public-private key pairs. Public-private key pairs are codes that are related to one another through a complex mathematical algorithm. The key pairs can reside on one's computer or on hardware devices such as smart cards or floppy disks.

Individuals or organizations must ensure the security of their private keys. However, the public keys that correspond to their private keys can be posted on Web sites or sent across the network. Issuers of digital certificates often maintain online repositories of public keys. These repositories make it possible to authenticate owners of digital certificates in real time. For example, publishers, as service providers, will want to authenticate the digital certificate of a faculty member or student in real time. This is possible by verifying the digital signature using the public key in the repository.

4. I understand that many campuses and services are using Internet protocol (IP) addresses or usernames and passwords, or both, to manage restricted access to resources. Why don't we continue using these techniques?

These two approaches—IP addresses, and usernames and passwords—have significant shortcomings.

- IP address authentication is increasingly difficult to maintain and does not accommodate remote access. Since an IP address identifies a machine, not a person, this technique is best used with very low-security applications.
- Username and password solutions do not scale, and they pose security risks. Passwords moving across the network as clear text can be read using public domain software and then misused. People often forget passwords, make all passwords the same, and share them. Passwords will continue to be used for network security and access control, but, increasingly, their use will be combined with other security mechanisms, or limited to very small user populations and low-risk applications.

5. How are certificates issued?

Digital certificates are issued by certificate authorities, just as state governments issue driver's licenses. There are several public companies in the business of issuing certificates. Also, many campuses are setting up their own certificate authorities and issuing certificates to their faculty members, staff, and students. This is similar to campuses issuing ID cards to the members of their communities. How campuses issue certificates will depend on the technical infrastructure and institutional policies that are established. Certificate authorities are responsible for managing the life cycle of certificates, including their revocation.

6. Why is the process of issuing digital certificates so important?

The process defines how a certificate authority establishes that a person or institution is who they say they are. Certification may require recipients to appear in person and to present pictures, birth certificates, or social security numbers. Certificates that are issued after rigorous authentication will be more trustworthy than certificates requiring little or no authentication.

Section Two:
Digital Certificate Infrastructure Requirements for the User

7. I have heard that Web browsers are an important part of the infrastructure for digital certificates. What is the relationship between the browser and the digital certificate?

- All major browsers come with the ability to store certificates and to deliver them to remote Web based applications.
- Digital certificates are part of the Secure Socket Layer (SSL) protocol, which enables secure electronic transactions on the Web.

8. How will students, staff, and faculty members receive their digital certificates?

Students, staff, and faculty members will receive digital certificates, usually on floppy disks or smart cards, from their institutions. Each certificate will verify the identity of its holder and confirm that he or she is a member or affiliate of the institution that issued the certificate. Certificates are usually valid for one to two years.

9. How many digital certificates is a student or faculty member likely to have?

Individuals will probably have several digital certificates with associated key pairs. One digital certificate may authenticate an individual as a member of an association. Others may authenticate a person as a customer of a particular bank or as a member of a campus community. Yet another might identify an individual to the federal or state government. Just as we carry many pieces of identification with us today, we are likely to have many certificates for use in cyberspace.

10. Where will faculty members and students store their private keys?

Individuals will be responsible for storing and protecting their private keys. Web browsers currently provide limited tools that do this for users. Individuals who use one primary machine, such as a laptop, will probably store their private keys on their computers. Individuals who frequently move from machine to machine, such as students, will probably store their private keys on small storage media such as floppy disks or smart cards.

Section Three:
Digital Certificate Infrastructure Requirements on the Campus

11. How does a campus prepare to set up a certificate authority on campus?

There are three major components of the public key infrastructure:

- *Certificate Authority (CA).* The CA provides all of the services required to issue, store, manage, and revoke certificates for an institution.
- *(LDAP) Authentication Database.* A lightweight directory access protocol (LDAP) database stores information about people and servers that have been authorized to receive certificates. Typically, the directory contains a unique identifier for the individual, associated demographic information, and, once the certificate is issued, the public key.
- *Attribute Server.* An attribute server is an optional component that may be used to exchange information that is not contained in a certificate but may be needed for authorization decisions.

Figure 1 illustrates that methods for access used on campus—Kerberos, passwords, and in-person ID—can be integrated with the digital certificate infrastructure.

Current methods rely on some form of directory service to authenticate a campus user for access to a service or resource. In this illustration, the University Directory Service is represented by the LDAP Authentication Database.

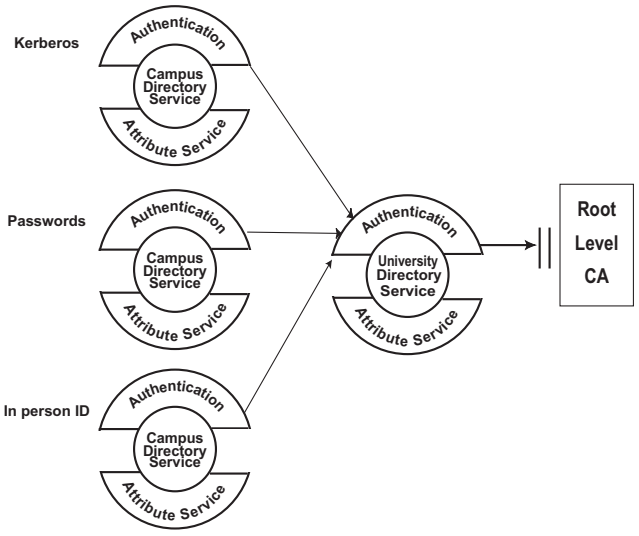

Fig. 1

12. What is in a digital certificate?

The contents of a digital certificate are prescribed by the X.509 standard, developed by the International Standards Organization (ISO) and adopted by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF). The latest version is now X509 v3. The principal elements of a digital certificate are as follows:

- Version number of the certificate format
- Serial number of the certificate
- Signature algorithm identifier
- Issuer of digital certificate: a certificate authority with URL
- Validity period
- Unique identification of certificate holder
- Public key information

13. Are there other characteristics of digital certificates—besides authentication and authorization—that would make digital certificates very attractive to libraries and publishers?

There is a subclass of certificates, called anonymous certificates, which allow researchers to search and retrieve information in privacy. Libraries have traditionally upheld, and researchers have come to expect, the right to privacy in research.

14. What is an example of the flow of information between a publisher's server and a user's computer in using digital certificates?

a. (See figure 2). The client attempts access to a controlled resource from a publisher, such as a database or digital library, usually through a Web interface.

b. The publisher's server asks the client to present a certificate.

c. The client presents a certificate, and the publisher's server verifies that the certificate
   - is issued by a recognized certificate authority,
   - asserts that the holder is a member of a licensed institution, and
   - has not been revoked.

d. The publisher extracts a URL from the certificate, which provides the means to retrieve from the campus or library additional information (attributes) needed for authorization decisions.

e. The publisher then connects to the specified attribute server using the prescribed secure protocol, presenting its own X.509 certificate to establish the secure connection. The attribute server verifies that the publisher's certificate is valid and uses the publisher's identity to determine access permissions from the information in the directory service.

f. The attribute server executes the query. The result of the query is presumed to be a list of attribute name-value pairs, including the service type or access authorized for the individual. The list of results is returned to the publisher.

g. The publisher looks at the value(s) of the "ServiceClass" attribute. If at least one value is valid for the publisher and service requested, the user is granted access. The precise access rights may depend on the ServiceClass attribute value(s), the institution to which the individual belongs, and other factors (e.g., number of current users).

15. How does a top root-level authority, such as CREN's, fit into the infrastrucutre?

The CREN certificate authority service is a top root-level service that issues certificates to organizational certificate authorities. CREN does not issue certificates to individuals. Top root-level certificate authority services establish a basis for trust among institutional participants, and between institutional participants and any non-educational entity with which they exchange information. This eliminates the need to establish multiple one-to-one relationships. More information about how to establish campus certificate authorities and how to obtain a CREN institutional certificate is available at http://www.cren.net.

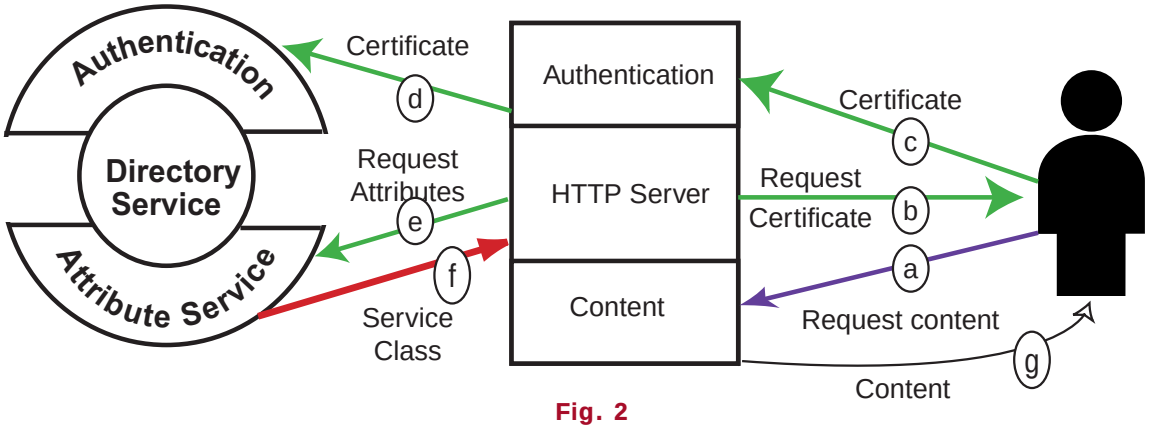

Fig. 2

articles and papers

Digital Library Federation. 1999. Prototype for Certificate-based Authentication. Paper presented at the Coalition for Networked Information's Spring 1999 Task Force meeting (April 26-27), Washington, D.C. Available at http://www.clir.org/diglib/dlfpresent.htm.

Feghhi, J. F., Jalil, and Peter Willliams. 1999. *Digital Certificates: Applied Internet Security*. Reading, Mass.: Addison Wesley Longman.

Jackson, G. 1998. Authenticating Users? What are the issues? *CREN TechTalk* (November 5). Available at http://seminars.cren.net/events/authenticating.html.

Karve', Anita. 1999. PKI Options for Next-Generation Security. *Network Magazine* (March) 30-35. Available at http://www.networkmagazine.com/magazine/archive/1999/03/.

Karve', Anita. 1999. Public Key Infrastructure. *Network Magazine* (November). Available at http://www.networkmagazine.com/magazine/archive/1997/11/9711sense.htm.

Lynch, Cliff. 1998. A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources, April 14. Available at http://www.cni.org/projects/authentication/authentication-wp.html.

Schiller, J. 1998. Certificate Authority Services. *CREN TechTalk* (October 8). Available at http://seminars.cren.net/events/caservices.html.

Wasley, D. 1999. Digital Certificates and Identification of Users on Campuses. *CREN TechTalk* (February 11). Available at http://seminars.cren.net/events/digicerts.html.

Web sites for general reference

Commonwealth of Massachusetts/ Information Technology Division, Legal Department PKI Site: http://www.magnet.state.ma.us/itd/legal/pki.htm.

Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates: http://internetcouncil.nacha.org/CARAT/.

Internet Council of the National Automated Clearing House Association (NACHA): http://internetcouncil.nacha.org.

JSTOR Discussion: http://www.jstor.org/about/remote.html.

MIT's Introduction to Certificates: http://www.ai.mit.edu/~mpf/ocean/java-beta/docs/guide/security/cert2.html.

National Institute of Standards and Technology (NIST). NIST is taking a leadership role in the development of a Federal Public Key Infrastructure that supports digital signatures and other public key-enabled security services. http://csrc.nist.gov/pki/.

Summary of Electronic Commerce and Digital Signature Legislation by the Information Technology and Electronic Commerce (ITEC) Law Department of McBride, Baker and Coles: http://www.mbc.com/ds_sum.html.

Thawte FAQ on Certificates: http://www.thawte.com/support/crypto/certs.html.

Verisign's Introduction to Public Key Cryptogrophy: http://www.verisign.com/repository/crptintr.html.

Corporation for Research and Educational Networking (CREN)

CREN is a nonprofit, member based organization that is dedicated to supporting the needs of networking and information technology professionals in the higher education community. Specific responsibilities of the organization include developing seminars, workshops, and educational and training materials that train faculty, staff, and students in strategic technology areas. CREN is deploying a top-level certificate authority service for the benefit of resource sharing among the higher education community.

1112 16th Street NW, Suite 600
Washington, DC 20036
phone: (202) 331-5366
e-mail: cren@cren.net
Web: http://www.cren.net

Digital Library Federation (DLF)

The Digital Library Federation (DLF) was founded in 1995 to establish the conditions for creating, maintaining, expanding, and preserving a distributed collection of digital materials accessible to scholars, students, and a wider public. The Federation is a leadership organization operating under the umbrella of the Council on Library and Information Resources. It is composed of participants who manage and operate digital libraries.

1755 Massachusetts Ave, NW, Suite 500
Washington, DC 20036
phone: (202) 939-4750
e-mail: info@clir.org
Web: http://www.clir.org/diglib/dlfhomepage.htm