Digital Certificates: How, Why, What to Do Next

By Gregory A. Jackson

My wallet is too thick with plastic cards, some of which replace keys—although I still have too many keys as well. More often than not, I have to use my wallet to locate the ones I have used to raise characters, to print charge slips. Now, instead, the magnetic strip on the back identifies me to credit bureaus and machines and opens doors and gates. On the Internet, not even plastic cards and magnetic strips will open many “doors” and “gates,” which instead require pure data: user names and passwords. My wallet and key ring are giving way to no-token identification and policy.

But no-token identification, like a key or card, can be unsecure. When I lose one of my physical keys or cards or give one to a parking attendant or waiter, whoever has it can be me, create a key and publish it, fraudulently. Such keys have three important properties. First, since they are based on large random numbers, they are effectively unique. Second, and critical to prevent impersonation, neither key can be derived from its mate. Third, if one key is used to perform certain calculations based on some text, then its mate can be used to confirm both that the first key was used to do those calculations and that the underlying text hasn’t changed. In effect, the first key signs the text, and the second key validates the signature, much as the second half of a message postcard would do. So Veronica gives one of her keys, the “public” one, to Archie. When she sends an e-mail to Archie later, she uses her “secret” key to perform the digital signature. When Archie receives the message, he uses Veronica’s public key, which he has gotten earlier, to confirm that her secret key signed the message and that the message is as she sent it. Although Archie can verify Veronica’s signature, he doesn’t have Veronica’s secret key, and so he can’t impersonate her.

Similarly, if Veronica has Archie’s public key, she can use it to encrypt her message to him, and only Archie, the sole possessor of his secret key, can decode the message. Archie personally received Veronica’s public key directly from her. This method of sharing public keys won’t work well on a large scale. But Veronica can publish her public key widely, in databases and on Web sites, because the public key can be used only to verify and not to create her signature. Now, then, can prospective correspondents with Veronica be sure that it wasn’t someone else, such as Betty, who created and published it, fraudulently, in Veronica’s name? Since Archie knows he has Veronica’s real public key, and since lots of people know Archie and have his public key, Archie can authenticate Veronica’s published public key by signing it. Jughead, who has Archie’s key, can sign Archie’s key. Now Jughead’s friends, who do not know Archie or Veronica but who do have Jughead’s key, have a chain of trust to Veronica. Alternatively, or in addition, everyone can agree on a common certifying authority that will sign each person’s key after verifying identity in some traditional way.

Managing digital certificates and keys requires policies, procedures, and systems to deal with trust, authority, revocation, and other issues. Collectively these constitute a “public-key infrastructure,” or PKI. Creating and managing a PKI is the principal challenge facing colleges, universities, and others that want to use digital certificates.

Who Benefits? Digital certificates substitute for physical presence and bypass the key-is-me problem. People can use electronic certificates to identify themselves unambiguously and safely, without physical tokens such as cards or keys. As institutional and individual transactions become more electronic, we must have mechanisms for identifying, authenticating, issuing, and revoking digital certificates. Third, they can be used to encrypt communications, which can then be decoded by only the intended recipient.

But outsourcing can be costly and restrictive and carry all the usual baggage: limited control, regression to the mean, holding contracts, and so forth. Some degree of external management may prove inevitable, for example, as the federal government moves to regulate businesses and industries. The preceding four decisions define the complexity of a campus PKI. The more complex the PKI, the more important will be the last decision.

5. Who does the work? The choice is between doing the work on campus and outsourcing it. Internal processes are highly controllable and can be as efficient as one’s resources permit. But staffing and managing them requires hard-to-find expertise and may entail liability if certificates are used externally. External processes turn staffing into someone else’s problem and can shift liability. But outsourcing can be cost-effective and restrictive and carry all the usual baggage: limited control, regression to the mean, holding contracts, and so forth. Some degree of external management may prove inevitable, for example, as the federal government moves to regulate businesses and industries.

Chops inked with cinnamon, signet rings pressed into wax, postcards torn in two, and notarial seals embossed in metal foil improve on simple scrawled signatures. In the same way, public-key infrastructures turn digital certificates into important, useful mechanisms for identifying, authenticating, and verifying electronic messages and messages. For those of us in higher education, as for Archie and his friends, the time for digital certificates and PKIs has come.

These important functions come at a cost. For example, certifying roles and permissions requires mechanisms for modification and revocation, and other issues. Collectively these constitute a “public-key infrastructure,” or PKI. Creating and managing a PKI is the principal challenge facing colleges, universities, and others that want to use digital certificates.

What Should Campuses Do Next? If digital certificates are to be used only among individuals, then commercial certifying authorities and software (Netcage, Internet Explorer, Outlook, Eudora, PGP, PGP, Verisign, Thawte, and so forth) provide ample support for exchanging signed and encrypted documents. But to use digital certificates effectively as an institutional tool, campuses must make decisions, develop policies, and implement a PKI. I’ll reduce the important decisions to five:

1. Will public keys certify status or authorization—for example, determine whether someone is a faculty member or can park in the library parking lot? If so, then the campus PKI must include mechanisms for issuing, modifying, and revoking keys. It also must include mechanisms allowing ensuring that accurate public keys are readily available and that secret keys remain secret but are properly backed up. These are also critical requirements if encryption (the next decision) is an institutional goal.

2. Does institutional business require encryption? If so, it is important to separate encryption keys from signature keys at the outset, to sign the former with the latter, and to ensure that secret encryption keys are available to the institution (this is “key escrow”) through the PKI. Secret signature keys, on the other hand, should never be known to anyone but their owners.

3. What departments and transactions will be encrypted? Most paper messages move around campuses by interdepartmental mail, often carried in unsealed envelopes by students. Their sole authentication is usually the letterhead on which they are printed. We must be careful not to demand more security and authentication for our electronic documents than is necessary. The substance of online transactions and the risk they present should determine the level of digital authentication, security, and encryption they require.

4. Who certifies whom? Colleges and universities must certify keys only for individuals who have proven their identity, proof that can be achieved centrally or departmentally. If colleges and universities want their certificates and keys to be recognized at other institutions, then some higher authority must sign them—perhaps a common certifying authority such as Verisign, perhaps the U.S. Post Office, or perhaps a higher-education consortium. (CREN is implementing such a service for its members; see <http://www.cren.net/ca/>.)

5. Where do we go from here? The choice is between doing the work on campus and outsourcing it. Internal processes are highly controllable and can be as efficient as one’s resources permit. But staffing and managing them requires hard-to-find expertise and may entail liability if certificates are used externally. External processes turn staffing into someone else’s problem and can shift liability. But outsourcing can be cost-effective and restrictive and carry all the usual baggage: limited control, regression to the mean, holding contracts, and so forth. Some degree of external management may prove inevitable, for example, as the federal government moves to regulate businesses and industries.

In September/October 2000, Greg Jackson, Chief Information Officer at the University of Chicago, wrote about public keys being available at <http://momadb.arch. edu/pgpkeys.html>.