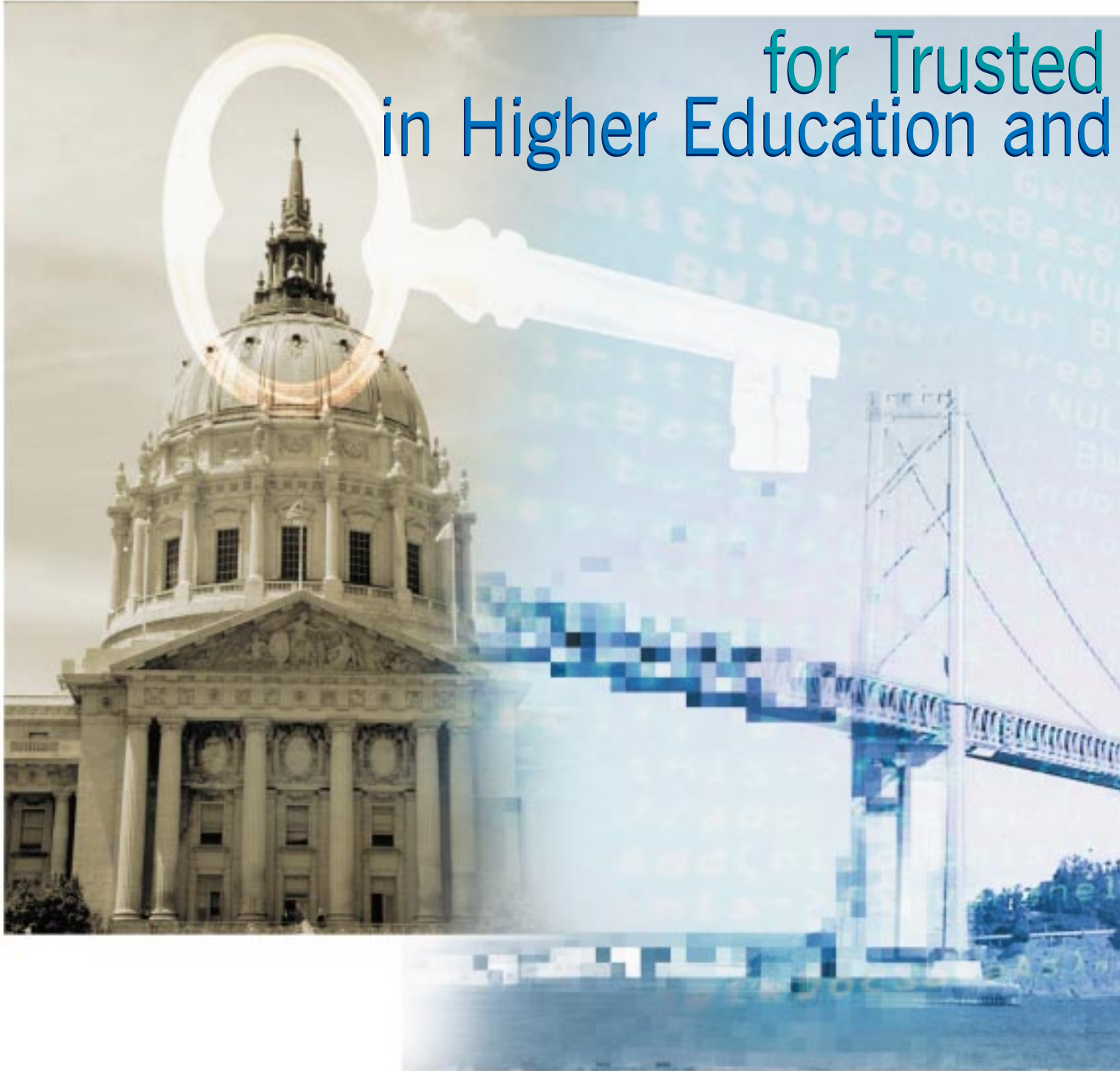


By Mark A. Luker

# ABRIDGE

for Trusted  
in Higher Education and



Campus networks and the Internet have enabled higher education institutions to dramatically improve many core functions through better communications. Education, research, and associated business transactions have benefited greatly from the open access offered to all members of the campus community and from the instantaneous, anywhere-anytime nature of network communications. Yet the results have fallen far short of the vision, with most campuses unable to take full advantage of their campus networks and the Internet to extend, speed up, and simplify their most important communications and procedures. Why?

*Mark A. Luker is Vice President of EDUCAUSE.*

# Electronic Communications the Federal Government



# The most fundamental basis of trust in communications is **knowing the true identity of the person or institution with whom one is dealing.**



One of the main reasons is that neither campus networks nor the Internet normally support the level of trust that is achieved through face-to-face identification, sealed documents, identification (ID) cards, ink signatures, witnesses, and the notary public. Such trust and assurance is absolutely required before colleges and universities can rely on the network for their most essential communications in education, research, and administration. Until it is achieved, higher education institutions must operate overlapping systems of electronics and paper and must incur the cost of unnecessary operations, wasted time, potential liabilities, and unrealized educational opportunities.

Traditionally, collections of user names and passwords have been used to provide trust through the network. These names and passwords are managed in an uncoordinated fashion by many different organizations: campuses, libraries, banks, and even online bookstores. Although this approach is better than nothing, the problems are numerous: it has many points of failure; it cannot support all the types of security and trust that are needed; and it is both difficult and very costly to manage. An alternative is the newer and fundamentally different approach called Public Key Infrastructure, or PKI. This technology *can* meet all security requirements and is now the leading candidate for implementing trust in large networks. A PKI provides the missing link that will allow a campus to “go electronic” even for those applications that require all the policy and legal commitments implicit in signed paper transactions and records. And PKI technology is now becoming available in off-the-shelf commercial products that can support a relatively straightforward and affordable introduction at the campus level.

Of course, the technology is just the starting point. Campus procedures and policies may well require reengineering to take full advantage of this new power. Yet a systematic switch to trusted electronic communications can pay very significant rewards in better access to the college or university (on campus as well as at a distance), flexibility of procedure and process, and efficiency in both time and dollars.

## **Trust in Electronic Communications**

The concept of trust in electronic communications can be broken down into five critical components of the assurance normally provided (or assumed) in traditional face-to-face and paper transactions: (1) authentication (identification); (2) authorization; (3) data integrity; (4) confidentiality; and (5) nonrepudiation.

The most fundamental basis of trust in communications is knowing the true identity of the person or institution with whom one is dealing. *Authentication* is the process that provides the additional information needed to reliably identify the party on the other end of the line. (I will refer to *authentication* simply as *identification* in the remainder of the article.) Traditional methods provide identification to the degree required by the task through such means as an ink signature that can be compared with verified originals on file, a “picture ID” card issued by a trusted third party, personal secrets (a password or mother’s maiden name), the seal of a notary public who has checked additional credentials, the signatures of witnesses, face-to-face recognition of business associates, call-backs to confirm the intent of the sender, fingerprints, or various combinations of such techniques. In many cases, trusted communications between strangers begin with the presentation of some form of

tamperproof certification stating that a trusted third party has performed a more complete identity check in the past. This is one of the major roles of the campus ID card, for example.

The next step after identification is *authorization*, or verification that a person has the legitimate authority to perform the requested activities. Authorization usually depends on roles and context. All students and faculty can check out books from the campus library. Only certain employees have the right to admit new students. Only the vice president for research can authorize a grant application to the National Science Foundation. Authorization for low-risk activities such as checking out a library book is often granted to all bearers of a special ID card, which may serve double duty for identification. Authorization for riskier activities usually depends on some stronger form of identification, followed by a check in an “authorization” database for prior permission to perform the activity.

Both identification and authorization are of little value (and indeed may be dangerous) if someone else can intercept and modify the message en route. *Data integrity* is an assurance that the content has not been altered. Data integrity has been provided to varying degrees in the past through the use of duplicate copies of signed pages, tamperproof sealed envelopes, sealing wax, trusted couriers, supervised fax transmissions, and special codes that can signal any change in content.

*Confidentiality* ensures that only the intended audience can read the message. This is absolutely critical in order to do the real work of a campus on the Net. Confidentiality has historically been achieved through a variety of techniques, ranging from sealed business envelopes to complex secret codes.



A final important aspect of trust is the expectation that the promises in a properly signed document can be enforced. This ethical and legal concept depends in part on *nonrepudiation*, the technical assurance that the document was actually signed by the indicated party. The traditional role of handwritten, personal signatures for this purpose can be bolstered with witnesses or other stronger means of identification if required by the situation.

Taken together, these five aspects of trust support the full range of legal and policy requirements for electronic com-

munications in higher education and elsewhere. It is clear that trust is not an all-or-nothing concept. It lives in a larger world of risk management that includes institutional policy, ethics, reputation, and insurance, as well as civil and criminal sanctions. Trust is usually defined in context according to acceptable levels of risk and can be strengthened at the cost of additional precautions if required. The challenge for a PKI is to provide trust in electronic communications without reliance on either face-to-face recognition or physical evidence and to do so in a practical and affordable manner.

### The Failure of Traditional Systems

Many institutional leaders may wonder whether the effort and expense required to implement a PKI is justified. Why not simply continue to rely on the traditional system of passwords to support electronic trust in the future? A hard-to-guess password that is known only to the owner can provide a good measure of *identification* and *nonrepudiation* if used through a secure communication channel. Passwords assigned to the users of a specific service, such as a licensed commercial database in the library, can provide *authorization* for its use. Encryption with secret codes can provide *data integrity* and *confidentiality*.

Unfortunately, as noted earlier, this approach is riddled with flaws. History abounds with sad examples of traditional password systems that fail in a regular and predictable manner. Passwords that are easy to remember are usually also easy to discover. Hard-to-remember passwords are often written down, where they are easy to steal. Con artists adept in the art of

“social engineering” regularly trick users into revealing their passwords. Although passwords sent to Web servers and other specialized applications can be protected through secure, encrypted communications, they are not safe in all applications and may be “sniffed” as they pass through the network “in the clear.” However it happens, even the strong suspicion of compromised passwords can completely negate all five components of trust.

A different problem arises from the fact that new computer applications are typically introduced to meet the needs of

functional areas, which often assign authorized users a new password for controlled access. A single professor, for example, may end up with a password for campus e-mail, one for a commercial database in the library, one for the campus financial system, one for the departmental computer, one for a federal financial aid system, one for grant applications to the Department of Energy, and so on, with all of this multiplied by the number of people involved. (Last week I heard once again the rueful complaint about too many passwords as I waited in line at an ATM machine.) This environment invites bad security habits that undermine trust.

The too-many-passwords problem will be multiplied in the future, when most members of the academic community are likely to participate in more types of trusted electronic communications. This trend is accelerating and is completely beyond the control of any campus. The federal government, for good reasons including a congressional mandate to reduce paperwork, is rapidly developing electronic systems to support most aspects of student financial aid. This will require trusted communications with the Department of Education, lending institutions, campus officials and financial systems, students, parents, alumni, the Internal Revenue Service, the Veterans Administration, and others. Trust will be required for electronic communications between multiple research-funding agencies and foundations, grant administrators, faculty members, graduate students, and the Immigration and Naturalization Service, among others. Nearly everyone involved in distributed learning programs will require some aspect of trusted communications. And of course there are all the administrative e-business transactions. These developments place both individuals and institutions in the

uncomfortable position of balancing increasing complexity and growing risks.

Last but not least, all this is very costly! The proper management of multiple systems of passwords is both troublesome and labor-intensive. One large university recently reported that over 40 percent of all work at the system help desk involves lost passwords. Each major functional unit pays to manage the computer accounts of its clients. To control legal and financial exposure, institutions must modify passwords and authorizations in a variety of systems every time a student or employee changes status. Important authorizations must be revoked immediately when a password is compromised. The institutional task of assigning and updating passwords for each person involved in each system gradually becomes unmanageable, costing increasingly more in staff for maintenance, exposing ever-greater risks, and ultimately limiting trust in the system. So, we’re now back where we started . . .

### **PKI to the Rescue**

A Public Key Infrastructure, or PKI, is a collection of technical services, policies, and business practices that can support the five critical aspects of trust across network communications. With a significant nod to oversimplification, a PKI solves the problems of human passwords by automating (1) the generation of very long, secure “keys” (to replace passwords), (2) the binding of personalized sets of keys to each individual, and (3) the automatic use of these keys in communications as required to provide the level of trust appropriate to the task at hand.

#### *Digital Certificates, Identifications, and Signatures*

The core technology of PKI depends on mathematical schemes that make it possible to issue tamperproof, electronic “certificates” that can be used to identify specific individuals and devices across computer networks. A certificate can be used much like a driver’s license or a campus ID card to provide a person with the additional level of identification required for important transactions. The underlying assumption is that the institution that issued the certificate “certifies” that it has performed a personal identification of



# A PKI can support all five aspects of trust on the network and can do so, if needed, to a degree of mathematical assurance that far surpasses traditional systems of ink and paper.



the individual, often requiring a face-to-face meeting with ink signatures, photographs, and additional corroborating evidence. Another assumption is that the person bearing the certificate is indeed the one to whom it was issued. The risks of this second assumption can be reduced by emphasizing personal responsibility (which can succeed if there are serious consequences involved, as in the case of credit cards), by issuing personal hardware tokens or “smart cards” that must be used to sign into the system, or if necessary, by utilizing biometric data such as retina scans and fingerprints. A third assumption is that the certificate is still valid when presented; validity can be addressed, as it is with driver’s licenses or credit cards, through procedures ranging from expiration dates to online validity checks.

The type of personal identification required for a transaction depends on the risks associated with a mistake. Checking out a campus library book differs from authorizing a million-dollar purchase, which differs from reading and modifying the grade records for a course. The identification systems required for each type of transaction are typically published in formal policy statements so that “relying parties” (i.e., those who must accept the identification) will know what degree of trust can reasonably be assumed. The trust decision usually depends on the reputation of the institution that issued the identification, the procedures that were used to identify the bearer at the time of issue, the difficulty of stealing or forging a passable fake identification, and the risks involved in the transaction. Digital certificates share all these considerations and can be tailored through policies and business practices to support a specific range of trust. Their great advantage over more

traditional means of identification is that they can be used safely and instantaneously across a computer network to establish identity without recourse to physical identifications.

Once identity is established in a PKI, the corresponding management of authorizations can be centralized in an “authoritative” campus directory that lists all members of the community along with their present roles (e.g., undergraduate student, state resident, temporary employee) and special permissions (e.g., access to the biology 101 lab room). Careful management of such a directory is dramatically easier and less error-prone than the corresponding task for multiple collections of passwords. Perhaps more important, the maintenance of roles and authorizations in an online directory means that a person’s digital identification can be used for many different transactions. Separate cards are no longer needed for each service, although there may be good reasons to use more than one. A change of role can be reflected immediately in the authorization database and does not require revoking an ID card. This conquers the complexity, risk, and cost multipliers for password systems.

The bottom line is that a PKI can support all five aspects of trust on the network and can do so, if needed, to a degree of mathematical assurance that far surpasses traditional systems of ink and paper. In particular, digital certificates can be used automatically with directories to present digital identifications and authorizations on demand and to attach binding digital signatures to electronic documents and communications.

### *Certification Authorities*

Where does a campus get the digital certificates required to identify its members? From a Certification Authority, or

CA. The CA manages the technical and clerical functions required to issue certificates according to the policies appropriate for the required level of trust. A critical component of the process is the actual identity-checking of the people or organizations to be certified. The office that issues campus ID cards is well suited to perform this task, as are other organizations such as a department of motor vehicles or a passport office. The corresponding campus directory is typically operated at a secure campus computer center and is generated from official information in the student and employee records. Technical operations for the CA either can be provided by a campus information technology organization using commercial products or can be outsourced to a number of vendors. The level of trust that can be placed in the work of a CA strongly depends on the policies that govern its operations. Taken together, these components can establish a campus PKI that can readily support a trusted electronic version of the majority of campus communications and transactions.

### *Barriers between Institutions*

One problem with ID cards is that they are issued by many organizations for their own purposes and may not be accepted or even readable outside the organization. Can a student’s ID card from one institution be used to check out a book from the library of another institution? The answer is yes, if an appropriate arrangement has been made in advance between the institutions, but in reality the answer is generally no. The ability to drive throughout the fifty U.S. states with a driver’s license from the licensee’s home state rests on such prior agreements.

Although there is agreement about general standards for the major compo-



nents of a PKI, the products of major vendors, not to mention their implementations on particular campuses, may differ in critical details. A complete system that works very well within a particular campus may not work to communicate with others outside the institution. It is highly unlikely, to say the least, that a single standard will arise to solve this problem in the near future, because this would require agreement among many independent academic institutions on a host of policy, technology, and business issues that have heretofore been defined only within the context of the campus.

A partial solution to using PKI between institutions can be achieved

through “hierarchical certification authorities” that arrange inter-institutional policy and technology relationships in the form of a tree, much like a family tree. Members of a family tree can trust the identity of their relatives because they can trace unbroken paths from child to trusted parent back to a common trusted ancestor. In a PKI, the trust relationships between “parent” and “child” nodes on the tree are spelled out in policy agreements that ensure that the procedures used at each node are acceptable to every other node. For example, the University of California (UC) is establishing a hierarchical PKI for the entire UC system. The UC Office of the President will be respon-

sible for the CA at the root of the tree and will issue authority certificates that vouch for a CA for each campus. All personal certificates will be issued at the campus level. Any campus can issue additional authority certificates that will vouch for CAs operated by its own major units, extending the tree to additional levels as needed.

Each major vendor of PKI services operates at least one hierarchy that can be joined by customers who want to use PKI without the investment of managing their own CA. Hierarchical CAs can greatly simplify the PKI environment for higher education by collecting campuses into large groups that can communicate with trust. Such CAs will not solve the whole problem, however, since there is little expectation that colleges and universities will ever succeed in reaching (or will even try to reach) all the policy and technology agreements that would be required to participate in a single hierarchy.

### **The Federal Bridge Certification Authority**

The U.S. government faced a similar situation in its need for trusted electronic



communications within and between its agencies. The “simple” solution of requiring each agency to adopt the same approach to PKI would not work, even in the government, since each of the agencies must make more or less autonomous choices in products and services for information technology according to its own needs, plans, budget, timing, and the market. The solution was to design a new service—called the Federal Bridge Certifi-

cation Authority, or FBCA. Opened for business in 2001, the FBCA in effect provides a common point of translation for critical PKI information from one agency to another.

The FBCA is concerned primarily with identification; it translates the level of assurance guaranteed by an ID card issued by one federal agency to the corresponding level of assurance in the ID-card language of another agency. With the FBCA, scientists at the Naval Research Laboratory can use their own electronic identifications (issued by the U.S. Navy) in trusted communications with colleagues at the National Institutes of Health (NIH), who can then be assured that these identifications represent a level of trust acceptable to the NIH. Staff members in the Office of Student Financial Assistance Programs in the Department of Education can use their own digital identifications to communicate with trusted systems in the Internal Revenue Service, for example, or in the Immigration and Naturalization Service. Members of the Armed Services can communicate with those in the Social Security Ad-

ministration and the Veterans Administration. A newly created federal agency can communicate with the others simply by joining the FBCA. An existing agency can even change its technology for PKI, as long as it remains in the FBCA.

The FBCA is not primarily about technology. Its most important role is as a formal organization that enables federal agencies to reach agreements, in advance, on how the PKI identification policies of

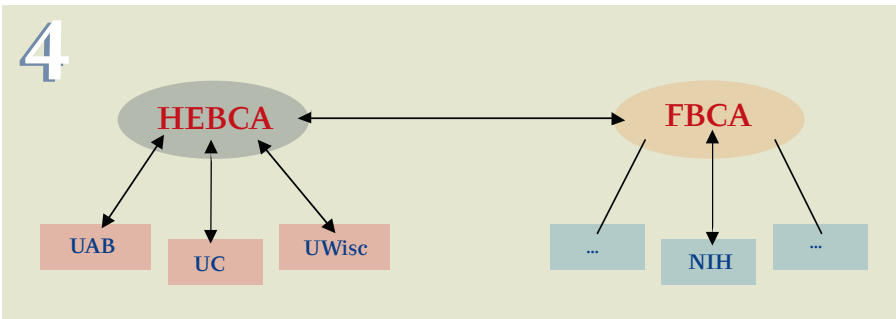
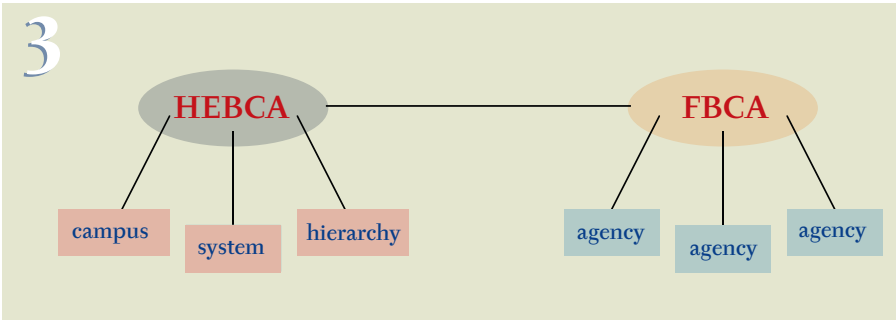
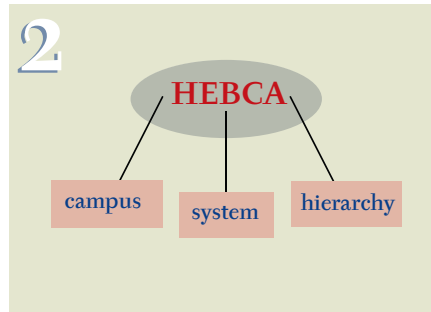
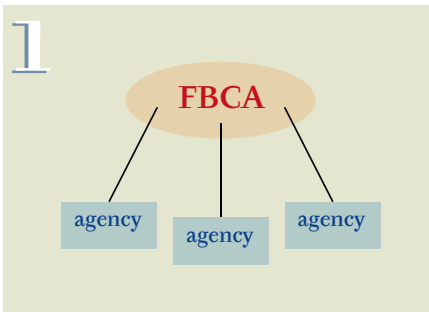
one agency will map onto those of another. These prior agreements then allow the trusted exchange of digital identifications by the thousands and millions. In addition, the FBCA dramatically streamlines the entire process of establishing these agreements by publishing FBCA model policies that cover the full range of topics ordinarily required in such agreements. With this approach, two federal agencies can agree to communicate with trust if they both meet the model policy standards of the FBCA. They do not need to separately verify that each is compatible with the other, a daunting process that would require on the order of  $N^2$  legal agreements between  $N$  agencies. (Just do the math!)

The FBCA requires a policy authority—accepted by all parties—that can govern the corresponding agreements. This is accomplished through the Federal CIO Council, which represents the top information technology leadership of each agency. The FBCA effectively cuts the Gordian knot for the agencies’ PKIs, allowing each agency to make its own choices for information technology within its own timetable, subject only to its agreement with the FBCA.

### **A Bridge Certification Authority for Higher Education**

Higher education campuses share many of the same characteristics of the federal agencies. But the higher education community is an even more complex collection of institutions that need trusted communications within and between campuses across a wide range of applications in education, research, and administration. Colleges and universities are even more autonomous in their choices of technologies, policies, and business methods and are even less likely to agree on the adoption of any single implementation of PKI. It is only natural, then, to propose the implementation of a Higher Education Bridge Certification Authority, or HEBCA, modeled on the FBCA, to facilitate trusted electronic communications within and between institutions of higher education.

Virtually every institution of higher education also has a need for trusted communications with multiple federal agencies on diverse issues including stu-



dent financial aid, taxes, grants administration, veterans' affairs, basic research, access to scholarly information, professional development, and education itself. For all the reasons mentioned above, it would be best to conduct such trusted communications with federal agencies using the same PKIs that are already in use on campuses rather than to use special-purpose passwords, keys, and other solutions designed separately for each case. Carefully linking the Higher Education Bridge with its Federal Bridge counterpart yields the potential benefit of trusted communications between all campuses and all federal agencies. This results in a tremendous win for both sides, as well as a dramatically simpler way to achieve the overall goals of each.

EDUCAUSE, the NIH, and the Federal PKI Steering Committee are presently supporting a demonstration trial of the HEBCA with the help of Internet2, the University of Wisconsin-Madison (UWisc), the University of

California-Berkeley (UC), the University of Alabama at Birmingham (UAB), Georgetown University, MitreTek, and several vendors of PKI technology. This trial is intended to show that the standard forms for grant applications to the NIH can be written and approved electronically by research faculty and grants officers at each of several campuses using campus-generated digital signatures, that these signed forms can be forwarded to the NIH by electronic mail, and that the NIH can then check the validity of all the signatures by automatically tracing the path back through the FBCA to the HEBCA to the campus directories. (Such trusted electronic communication of signed documents is of serious practical interest to the NIH, which receives and processes multiple paper copies of some forty thousand grant applications each year.)

At the big-picture level, this demonstration should show the feasibility of using PKI for trusted communications in

a wide variety of applications between any campus in the HEBCA and any federal agency in the FBCA. The simpler case of trusted communications between campuses can be handled through the HEBCA alone.

### A Policy Authority for the Higher Education Bridge

One important way in which the analogy between higher education and the federal government breaks down is in terms of governance. There is no counterpart of the Federal CIO Council in higher education. Yet there is a similar need for an authoritative body that can govern policy for the HEBCA. For this reason EDUCAUSE, representing the information technology leadership of higher education, has received the support of the American Council on Education, representing the executive leadership, and the National Association of College and University Attorneys, representing the institutional legal officers, to form a policy board with the de facto authority to support the implementation of a Higher Education Bridge. Depending on the outcome of the present trials, the HEBCA itself will be implemented under EDUCAUSE management with the help and participation of PKI experts in EDUCAUSE Net@EDU, Internet2, the federal government, and EDUCAUSE corporate partners and member institutions.

### Conclusion

The development and testing of a Higher Education Bridge Certification Authority signals a promising new approach to trusted electronic communications across the academic community. At the same time, the two-way link between the Higher Education Bridge Certification Authority and the Federal Bridge Certification Authority reflects an important new sphere of cooperation between higher education and the federal government. In the months and years to come, both this new approach and this new cooperation can be used to sketch a roadmap for the development of trusted electronic communications, allowing higher education institutions to take full advantage of the opportunities offered by their campus networks and the Internet. *e*