

PKI: A Technology Whose Time Has Come in Higher Education

The importance of securing networks and network services at higher education institutions has never been higher than it is now. The costs of security incidents continue to escalate, government regulations require increased vigilance, and hackers are as prolific as ever. Meanwhile, users and institutions demand more network services and the exchange of more potentially sensitive information within these services. Public Key Infrastructure (PKI) is emerging as a viable overarching technology to address security requirements in higher education and elsewhere. The PKI Lab at Dartmouth College has two years of experience in investigating and deploying PKI on campus and, with Andrew W. Mellon Foundation support, seeks to help other colleges and universities deploy PKI.

What Is PKI?

PKI encompasses comprehensive security technologies and policies using advanced cryptography and international standards to provide fundamental computing infrastructure improvement. PKI enables

- user authentication that is stronger than traditional “passwords on servers” mechanisms;
- digital signing of e-mail and other documents for proving the originator’s identity, for verifying document integrity, and for streamlining paper-free business processes; and
- encryption to protect critical e-mail and other data in a user-focused manner.

Point solutions exist for each of these features, but only PKI addresses all features well with standards and broad industry support. Robust services and commercial and open-source tools provide a sound PKI foundation. Browsers, Web servers and services, e-mail readers and list-servers, database servers, PDF readers, VPN appliances, WPA wireless authentication, USB keys, and smart cards all have integrated PKI support. Because PKI is standards-based, they can all interoperate with each other.

PKI uses asymmetric key-pair encryption. The only way to decrypt data encrypted with one key in the pair is by using the other key in the pair. Users and servers have industry-standard certificates to associate their key pairs with their identity and other information, such as the authority that issued the certificate and allowed uses of the certificate. Certificate Authorities (CAs) issue PKI certificates and attest to the validity of the identity specified by the certificate. Operating systems, applications, hardware add-ons, and servers all support PKI certificates and keys. PKI enables trust between two or more parties (possibly from different organizations or nations) without prior knowledge of one another.

The Need for PKI Now

The need for improved cybersecurity is apparent. Higher education IT staff and systems are besieged by hacker attacks, viruses, and spam. College and university networks tend to be very open and exposed to attack, and their users tend to exhibit risky behavior. A PKI Lab survey of 171 Dartmouth undergraduates revealed that 75 percent of them shared

their password and that fewer than half of those changed their password after sharing. In fact, nearly two-thirds of them *never* voluntarily change their password regardless of how they use it and despite recommendations to do so. PKI’s strengths directly address this and many other security challenges faced in higher education.

Yet despite its advantages, PKI has not been widely deployed in higher education due to

- the high expense and complexity of implementing the infrastructure;
- the unavailability or poor implementation of application support for PKI;
- the lack of critical mass; and
- the accepted adequacy of other solutions (such as name/password or IP address authentication).

Today, servers, services, and tools for implementing PKI are less expensive and more robust. PKI infrastructure is mature and is ready for extensive adoption. Applications have lagged behind and still need refinement, but they are steadily improving and will improve more rapidly with increased user demand and feedback. Name/password and IP address authentication no longer provide adequate security and flexibility: new technologies, increased “bad guy” sophistication, a larger number of services for each user, and higher usability expectations together render them less secure, more expensive, and/or less satisfactory to users than a comprehensive PKI solution.

PKI needs intra-institutional (and potentially inter-institutional) technical and

administrative commitment and requires more policy and operational overhead to get started. But once established, PKI yields economy of scale, ease of use, and interoperability benefits far beyond those of competing solutions. PKI is more secure and is new, so implementing PKI costs more initially than keeping the status quo but will cost less in the long term because the status quo exposes risks and incurs inefficiencies far more expensive in the long run. The key is to overcome initial PKI adoption hurdles, and now is the time for higher education institutions to start doing so.

Global use of PKI in higher education will enable increased information sharing and technological collaboration in a much more pervasive fashion than is possible today. PKI allows secure and controlled sharing of intellectual property, research, and teaching materials. PKI adoption hurdles are lower than ever, and the benefits are greater than ever. The time has come to stop studying and testing and to take the plunge.

PKI Deployment Success at Dartmouth

Over the past year, Dartmouth's PKI Lab (<http://www.dartmouth.edu/~pkilab>) has deployed PKI into ever-wider production for both students and staff. We focused initially on infrastructure, in particular our own Certificate Authority (CA) using commercial software and our existing LDAP service, to enable Dartmouth users to self-enroll for PKI certificates via a secure Web enrollment page. Our thorough user Web site (<http://www.dartmouth.edu/~pki>) introduces users to PKI and guides them through enrollment. Early applications (Banner Student Information System, library electronic journals, the business school portal) allow PKI authentication in place of Kerberos or other "password/username across the wire" authentication techniques.

The PKI Lab is working on enabling more applications, including the VPN concentrator, the wireless network, software downloads, and Blackboard. We will continue to motivate people to use PKI authentication until it is the only option for most of them. We intend to aggressively deploy large numbers of hardware tokens to hold users' PKI credentials

more securely, provide two-factor authentication, and facilitate mobility. Our S/MIME e-mail pilot projects succeeded, and we plan to implement S/MIME widely. We issue identity certificates for our internal network servers and appliances.

We succeeded in making enrollment and the use of PKI credentials very easy. All our PKI users self-enrolled, with almost no involvement from support staff (though support staff were trained beforehand so that they would be prepared). Our systems steer users with old, PKI-unfriendly browsers to alternate authentication mechanisms. The smoothness of our initial deployments has repeatedly caused us to accelerate our plans for additional applications and larger numbers of users.

Throughout our PKI investigations and deployment, we are diligently documenting our findings and publishing our experiences to the Web for all to use. We report and fix, or work around, PKI implementation problems with applications and application servers. We cultivate collaborations with key PKI vendors to aid them in improving their products and to assist them in better meeting higher education requirements. These efforts will help keep the costs incurred by future higher education PKI adopters far lower than the costs incurred by Dartmouth. The benefits an institution will reap in the form of "security breach incident" avoidance, improved user productivity, and streamlined business practices will, in the medium to long run, far outweigh the cost to plan, design, and implement PKI.

Future Development in PKI

As PKI matures and gains wider deployment, higher education organizations will seek to create ambitious inter-institutional infrastructures to help realize PKI's promise of inter-institutional user-level trust capabilities. The potential for streamlining operations, expanding collaboration, and sharing services is enormous, both among schools and with government. EDUCAUSE is sponsoring the Higher Education Bridge Certificate Authority (HEBCA) to allow campuses to trust users' digital credentials issued by each other's PKI authori-

ties and to allow interoperability with the Federal Bridge Certificate Authority (FBCA) for digitally signing documents such as grant proposals and student loan transactions. Internet2 is establishing a US Higher Education Root (USHER) Certificate Authority for more-traditional hierarchical trust models—to provide server identity certificates for traditional services and to enable Shibboleth federations among schools and with vendors (Shibboleth also can use PKI as one of its options for on-campus user authentication). The Higher Education PKI Technical Advisory Group continues its leadership role in defining how PKI fits in higher education, and an EDUCAUSE (Net@EDU) PKI for Networked Higher Education working group focuses on publishing case studies of schools with deployments of PKI credentials to end users. The Organization for the Advancement of Structured Information Standards (OASIS) PKI Technical Committee helps vendors enhance and refine their PKI offerings to facilitate further adoption.

PKI offers unique solutions to real problems. With extensive deployment in the federal government and among notable industry giants, a sound foothold in higher education, and significant new developments such as HEBCA and USHER, the future for PKI in higher education looks bright indeed.

Note

See <http://www.dartmouth.edu/~deploypki/> for more information about deploying PKI in higher education. The PKI Lab is currently seeking several colleges or universities that would like to become early PKI adopters and with whom we can collaborate in this process.

Mark Franklin is Project Manager in the PKI Lab at

Dartmouth College. Larry Levine is Director of Computing at Dartmouth College. Denise Anthony is Assistant Professor of Sociology at Dartmouth College. Robert Brentrup is Associate Director of Technical Services at Dartmouth College.

