Public Key Infrastructure and Higher Education: An Introduction

A Publication of the Postsecondary Electronic Standards Council
Washington, DC
May, 2000
# Table of Contents

Credits.................................................................................................................iv

Executive Summary............................................................................................v

1 Introduction.........................................................................................................1
  1.1 The Purpose of Public Key Infrastructure (PKI)...........................................1
  1.2 Understanding Public Key Infrastructure and Technology.........................2
      Cryptography Overview
      Digital Signatures and Public Key Encryption
      Where Does Infrastructure Come In?
      PKI Process Flow
  1.3 Policy – The PKI Document Set.................................................................4
  1.4 Models of PKIs............................................................................................5
      Closed Model (Enterprise Model)
      Network Model (Community of Interest Model)
      Open Model
  1.5 A PKI Model for Higher Education............................................................6
  1.6 Reference URLs.........................................................................................7

2 The Use of PKI in Education and Other Industries........................................8
  2.1 The University of Texas System (UT) – Closed Model............................8
  2.2 University of California (UC) – Closed Model...........................................9
  2.3 Automotive Network eXchange (ANX) – Network Model.........................10
  2.4 The Digital Library Federal – Network Model...........................................11
  2.5 GSA ACES – Open Model..........................................................................11
  2.6 ABA Trust ID® Program – Open Model...................................................12

3 Issues in Deploying and Using Public Key Technology in Higher Education..................................................13
3.1 Acceptance by Consumers ................................................................. 13
   Access to the Technology
   Ease of use
   Technical Support

3.2 Trust ........................................................................................................... 13
   Confidentiality
   Privacy

3.3 Interoperability .......................................................................................... 14
   Standards
   Technical interoperability
   Policy Interoperability
   Other Interoperability Initiatives: Federal Bridge CA and NACHA

3.4 Key Storage ............................................................................................... 15

3.5 Certification Authority Services ............................................................... 16
   Technology Knowledge and Implementations
   Policies and Procedures
   Data Processing and Facility Requirements
   Risk and Liability
   Applications Supported
   Customer Support

4 Work Group Recommendations .................................................................... 19
PKI Work Group Members

David Leonard, USA Group, Chair
John Barkley, NIST
Andrew Boots, US Department of Education
Michael Capps, Ed Fund
David Garver, ScienceWise
Dan Geller, NCS
Casey Lide, EDUCAUSE
Kelly Newcomb, TGSCL
Jan Nielsen, Campus Pipeline
Wally Reeves, University of Texas at Austin
Pat Salava, Educational Testing Service
Michael Sessa, NASLA
Paul Soohoo, Educational Testing Service
Shelby Stanfield, University of Texas at Austin
Craig Yamamoto, Ed Fund

This document was produced by members of the PKI Work Group in collaboration with technical consultants from Digital Signature Trust

Keren Cummins, Vice President, Government Services
Debbie Blanchard, Sales Engineer
Louis Jurgens, Sales Manager
Tim Pinegar, Senior Engineer

The Chair wishes to give special recognition to Work Group members Andy, Dan, Casey, Wally, and Paul and staff members Betsy and Andrew for their contributions.

~

The Postsecondary Electronic Standards Council
One Dupont Circle, NW, Suite 520
Washington, DC 20036
(202) 293-7383
http://www.StandardsCouncil.org

© May 2000
Public Key Infrastructure and Higher Education: An Introduction

Executive Summary

The Postsecondary Electronic Standards Council (PESC) created a Public Key Infrastructure (PKI) Work Group to determine how PKI can serve the needs of the higher education community. In this paper we examine the purpose of PKI and how it works in general, show how it has been implemented to date in higher education and elsewhere, discuss various models of PKI and the issues involved in an open PKI system, and present our recommendations for PESC support of PKI in higher education.

Introduction

PKI can provide assurances that data sent electronically over open networks arrive unaltered, unseen by unauthorized persons, from an authenticated sender who cannot deny sending the data. Without some or all of these assurances, there is not the required secure environment for many electronic transactions to take place.

As students, schools, lenders, service providers, and state and Federal agencies move from paper to electronic data exchanges of student data over the Internet, security concerns become important not only to the senders and receivers of this data but also to the public at large. Federal laws, regulations, and trading partner requirements for providing security with traditional paper processes and limited electronic exchanges must be adhered to in electronic data exchanges in an open environment. Digital signatures and encryption achieved through the use of a PKI can satisfy the required security attributes.

Discussion

A PKI, based on asymmetric or public key cryptography, incorporates the hardware, software, policies and procedures that allow previously unknown parties to exchange data in a secure environment. Two PKI models—closed (or enterprise) and network (or community of interest)—are found in use in various industries. A third model—open—is still in the conceptual stages. When fully realized, it will make available a “portable Internet credential” with broad utility even outside the originating community. The PESC community, with its singular focus on the entire higher education enterprise, is broad enough to feel the need for the open model PKI.

Individual universities and university systems are establishing their own closed PKIs to allow students, faculty, and administrators to use information technologies to improve the way they accomplish their business. Review of other network and open models such as the US General Services Administration ACES project and the American Bankers Association TrustID initiative, provide examples for higher education to consider in the move from institutional closed PKIs to an eventual network and open PKI.

Challenges for implementation of a broader-based PKI in higher education revolve around acceptance of the technology by users, trust in the process, interoperability, the issues surrounding provision of certification authority services, and costs.

Recommendations

The PESC PKI Work Group recommends that PESC encourage electronic commerce in higher education by fully supporting and promoting the use of PKI. Its role would focus on research and sharing of technical, legal and policy information with members of the higher education community and on the cooperation with existing and new initiatives to employ PKI technology in higher education. The Work Group recommends a standing committee be formed and a PKI expert be engaged to provide appropriate information on the topic on a continuing basis.
1 Introduction

The revolution in the delivery of services through electronic means that is taking place in the commercial and government worlds has a special resonance for the higher education community -- a community that exists entirely for the communication of knowledge and information. The Postsecondary Electronic Standards Council (PESC) comprises a diverse group of organizations that have entered into partnership within the higher education community for the purpose of improving service and controlling costs through the promotion of standards for data sharing.

The higher education community and those that support it--campus administrative offices, testing services, financial aid lenders, servicers and guarantors, and state and federal agencies--are finding more ways to provide better service and cut costs by taking advantage of electronic delivery of computerized data. As paper processes are replaced by electronic data sharing, current and potential trading partners must agree on data formats, code sets, encryption schema, and other standards to facilitate the flow of information. To that end, the PESC Public Key Infrastructure (PKI) Work Group was charged to investigate industry, state, and federal efforts to establish and regulate public key infrastructure (PKI) components of public key cryptography, digital signatures, digital certificates and certification authorities for secure Internet data exchanges.

This paper is intended to examine, from the perspective of the PESC, how PKI, or public key infrastructure, can provide a cornerstone for furthering that revolution in the higher education community. The paper will examine the purpose of PKI and how PKI works in general; how PKI is working in current implementations in higher education and elsewhere; what special concerns higher education may need to address in the future; major issues in the implementation of PKI in an open system, and the Work Group’s recommendations for further action by PESC.

1.1 The Purpose of Public Key Infrastructure (PKI)

In the conventional world of business and professional communications, basic assumptions can be made when a transaction is conducted using original signed documents, delivered in sealed packages directly to the participating parties. Generally, organizations that use the public network to transmit business communications must understand with whom they are dealing; that no one has altered the content of the communication after it was signed; that no one unauthorized has seen the information; and that the signer of the document cannot deny having sent the document. These are the fundamental assurances that make transactions between remote parties possible.

Simply stated, the most fundamental purpose of a PKI – a public key infrastructure – is to provide these same types of assurances about the content and parties to transactions that take place over an open network, sometimes among parties not otherwise known to each other. By enabling the use of digital signatures and encryption, PKI can provide the same four basic security services for today’s data transmissions:

- **Authentication** — Ensure that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information.
- **Data Integrity** — Ensure that data is unchanged from its source and has not been accidentally or maliciously altered.
- **Non-repudiation** — Ensure strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient), and, to the recipient, of the sender’s identity, sufficient to prevent either from successfully denying having sent or received the data. This includes the ability of a third party to verify the integrity and origin of the data.
- **Confidentiality** — Ensure that information can be read only by authorized entities.

In addition, PKI can also offer additional security services not offered by a paper process, including:
• **Authorization** — Ensure that the user, either sender or recipient, is authorized for access to data, systems, or applications

• **Availability** — Ensure that legitimate users are not unduly denied access to information and resources

The term “public key infrastructure” or “PKI” refers to a complex suite of hardware, software and particular cryptographic components, combined with adherence to policies and procedures that enable business applications to operate in a secure environment. The particular cryptographic components used are those of public key, or asymmetric, cryptography. To discuss how PKI can serve higher education it is fruitful to review how those technologies, particularly digital signatures, actually work.

### 1.2 Understanding Public Key Infrastructure and Technology

To understand a PKI, it is important to understand how public key technology is used to encrypt and sign an electronic message. A digital signature is not a digitized image of a handwritten signature, nor is it a PIN or a password. Rather, a digital signature is an attachment to an electronic message that includes a mathematical digest of the message, created using public key cryptography. As a result, a digital signature is specific both to the signer of an electronic document or message as well as to the electronic document or message itself. Thus, a digital signature can be used to affirmatively identify both.

**Cryptography Overview**

There are two fundamental types of cryptography, symmetric cryptography and asymmetric or public key cryptography. Each of these cryptographic systems has distinct characteristics and is used in different ways to provide general security services.

Symmetric cryptography is the most familiar. It is based on a shared secret, or key, and works well within isolated environments. A simple example of symmetric cryptography is seen when children create a "secret code" by converting all the letters of the alphabet to their numeric equivalents, 1-26, and then adding, say, the number five. The child receiving the secret message has only to subtract five from each number in order to be able to reconstitute the correct numbers for the original message. The shared secret is the number five. In real commercial uses of symmetric cryptography, the algorithm used to encrypt may be enormously more complex. The challenge is communicating a secret key between the sender and receiver without anyone else finding out, because anyone who might intercept the key would be able to read, modify, or forge messages that were encrypted or authenticated using that key.

The inherent problem with symmetric cryptography is one of scalability. In order for the communications to be confidential, the exchange of a key, or shared secret, must be done securely between every pair of participants. Obviously, this type of secure distribution becomes increasingly difficult as the number of different people with whom you want to communicate securely grows.

The other encryption technique is asymmetric or public key cryptography which involves an asymmetric key pair. This key pair comprises what is referred to as a public key and a private key. The public key, as its name suggests, may be freely disseminated. This key does not need to be kept confidential. The private key, on the other hand, must be kept secret. The owner of the key pair must guard his private key closely, as sender authenticity and non-repudiation are based on the signer having sole access to his private key. Furthermore, there is no longer a need for the parties to a transaction to exchange any secret information.

There are several important characteristics of these key pairs. First, while they are mathematically related to each other, it is impossible to calculate one key from the other. Therefore, the private key cannot be compromised through knowledge of the associated public key. Second, each key in the key pair performs the inverse function of the other. What one key does, only the other can undo.
Digital Signatures and Public Key Encryption

Digital signatures are created using asymmetric or public key cryptography. The sender can produce a one-way hash of an entire message or a synopsis of the message. The sender encrypts the hash with their private key, thereby signing the document. When the message is received, the receiver recreates the message’s hash from the message he received using the sender’s public key. If this process produces an identical result, then the recipient knows the following:

- that the person who sent the message is the holder of the private key associated with the public key used to verify the message;
- that that person cannot deny having sent the message;
- that the message has not been altered or modified in transit

If the sender also wishes to encrypt the message so that only the receiver can read it, instead of using his own key he must retrieve the public key of the intended receiver. Encryption conducted with that key is one-way, and only the private key of the intended receiver can be used to decrypt the message. Luckily, most PKI-enabled applications (e.g., S/MIME email) perform all of this “cryptomagic” for the user automatically.

Where Does Infrastructure Come In?

While the public key technology described to this point is available and in use, there are still shortcomings – at least from the standpoint of secure transactions among strangers. As seen from the example above, in order to validate a digitally signed document, the recipient must have access to the signer’s public key. Likewise, in order to encrypt a message to a specific recipient the sender must have access to that recipient’s public key. How is this obtained?

The signer may provide it directly, but there are two problems with this method. First, it is not a scalable solution. Taking into account the millions of Internet transactions among relative strangers, it is not realistic for all users to mail their public keys to everyone with whom they want to do business. Second, there is the risk of identity fraud. If the signer sends you a public key claiming to belong to John Doe, how do you know that it really was issued to John Doe?

The question arises: Who will attest that a particular public key really belongs to a specified individual? The use of public key technology creates the need for an entity to serve as a trusted third party (TTP) to vouch for individuals’ identities and their relationship to their public keys. This entity, in public key infrastructure terminology, is referred to as a certification authority, or CA.

The CA is a trusted third party that issues digital certificates to its subscribers. The digital certificate is the document that binds a person’s (or entity’s) identity to the key pair used to digitally sign electronic communications. Digital certificates contain the name of the subscriber, the subscriber’s public key, the issuing CA’s public key, and possibly other pertinent information about the subscriber. The digital certificate is signed by the issuing CA, so that the information in the certificate cannot be altered. They can be revoked if the private key becomes compromised, or if there is some other change to the accuracy of the identity information, such as separation from an organization.

Certificates are typically stored in an on-line, publicly accessible repository. In addition to valid certificates, the repository also maintains an up-to-date listing of all the unexpired certificates which have been revoked.

What might these relationships look like over time? On a periodic basis, perhaps annually, a subscriber applies to a certificate authority (CA) for a digital certificate. The CA verifies the identity of the subscriber and issues the digital certificate. The CA publishes the certificate to a repository. Then for each transaction, the subscriber can now use the private key of the digital certificate to sign electronic messages.
Relying parties can now receive the message, verify the digital signature with the public key of the subscriber, and check the repository for validity and status of the digital certificate of the subscriber. The following figure, *PKI Process Flow*, highlights this process.

**PKI Process Flow**

Step 1. Subscriber applies to Certification Authority for Digital Certificate.
Step 2. CA verifies identity of Subscriber and issues Digital Certificate.
Step 3. CA publishes Certificate to Repository.
Step 4. Subscriber digitally signs electronic message with Private Key to ensure Sender Authenticity, Message Integrity and Non-Repudiation and sends to Relying Party.
Step 5. Relying Party receives message, verifies Digital Signature with Subscriber’s Public Key, and goes to Repository to check status and validity of Subscriber’s Certificate.
Step 6. Repository returns results of status check on Subscriber’s Certificate to Relying Party.
Step 7. The Relying Party now can make an informed decision as to whether or not to trust the subscriber's message.

Properly configured, today's browsers and other PKI-enabled clients make these steps practically seamless to the participants involved.

The Repository plays a similar role in encryption of an electronic message so that the confidentiality of the message content is maintained. The subscriber encrypts the message with the Relying Party’s public key. Only the Relying Party can decrypt the message with his private key.

**1.3 Policy – The PKI Document Set**

Published documentation for a certificate authority articulates the measures taken by that certificate authority to authenticate certificate subjects, such as users, servers, and organizations, and to protect the certificate authority. The minimal set of documents to be prepared by the certificate authority is the Concept of Operations (ConOps), Certificate Policy (CP), and Certificate Practices Statement (CPS). The CP and the CPS are typically published and are essential for any certification authority to define the technical, procedural, and legal foundations contributing to the trustworthiness of the certificate authority. To ensure the integrity of a PKI environment, a process must be established to verify compliance with these policies and practices. Each of these documents is described in the following sections.

**Concept of Operations**

The Con Ops is a high level document describing policies and basic concepts of operation unique to the participating organization's requirements and how the application of PKI technology would work. A Con Ops document includes a survey of existing business practices and highlights areas where change may be
needed to accommodate digital signature implementation. Additionally, the Con Ops would include an overview of the proposed system design and architecture.

**Certificate Policy**

The CP provides the fundamental grounding and basis for all PKI-related implementations, including applications. It is a detailed description of the operating rules surrounding the implementation of digital certificates. The CP typically addresses: the community of users involved; appropriate uses of certificates; obligations of all parties; publication of certificates; privacy and confidentiality provisions; general requirements for CA operations including application procedures; identification and authentication; certificate issuance; certificate acceptance; renewal, rekey, and revocation of certificates; and other legal provisions. It also includes a detailed description of digital certificate format at the syntax level. The format is tailored specifically to meet the operational requirements of the participating organizations as described in the Concept of Operations (ConOps).

**Certificate Practices Statement**

The CPS is a public statement of the practices for issuing and validating certificates and for supporting reliance on certificates. Based upon the guidelines provided by the CP, the CPS is designed to be a simple and straightforward explanation of how the system works and to what standards the operations of the CA may be held by the participants. It includes a detailed description of the identity proofing process, certificate issuance and validity period, and certificate revocation procedures and maintenance. This is the working document that describes every facet of digital certificate policy, generation, use, and maintenance.

### 1.4 Models of PKIs

The Federal Government, in *Access with Trust*, describes PKI as

> a combination of products, services, facilities, policies, procedures, agreements, and people that provides for and sustains secure interactions on open networks such as the Internet. It is not necessarily a single monolithic entity. It might be a distributed system in which the component elements may include multiple public key infrastructures which are interoperable and interconnected.

The unifying element of a PKI is the certificate policy, which describes the community using the PKI, eligible applications supported by it, and the rules of engagement that all parties must follow. In the context of the statement above, then, there are three primary models of public key infrastructures that are worth reviewing in the context of higher education. They differ with respect to the character of the overall community or communities served, and, consequently, with respect to the nature of the policy authority needed to create and administer the certificate policy. These models are: Closed or Enterprise Model, Network or Community of Interest Model, and Open Model.

**Closed Model (Enterprise Model)**

Some communities are, by their nature, self-contained with their own well-defined policies. The typical example given is a business in which its employees and management would represent such a self-contained community. In this scenario policies pertaining to identification and authentication of employees, storage of private keys, management of the CA, and so forth can be dictated by the management. In the “closed” scenario, the PKI policies, practices and procedures are of interest only to the local community served. In the closed model, a unit of the enterprise’s management organization plays the role of policy authority.
**Network Model (Community of Interest Model)**

There are also communities that can best be described as a union or conglomeration of multiple distinct communities. Industry associations and trading partnerships are both examples of such communities of communities. For instance, the Automotive Network Exchange (ANX) is a network of independent companies that do business together in the automotive market. Another example might be the Digital Library Federation. In the network scenario, a group of organizations come together to collectively identify the policies, procedures, security services and applications that will be supported by their PKI. A PKI deployed to support the interactions between members of such extended communities is defined as a “network” model. The policy authority can be a pre-existing body, as in the case of the ANX, or can be a body created by the participants specifically for the purpose of managing the PKI. The Digital Library Federation is an example of this model and is discussed in the next section.

Plans for network or community-of-interest PKI's in higher education typically center around functional areas like the administration of student financial aid -- a group that represents a subset of all students; a subset of administrators; plus external entities like the Office of Student Financial Aid and financial institutions.

**Open Model**

Some communities are very broad in nature, and may be associated with policies that are either informal, or largely specified in regulations and legislation. Some examples are the community of all retail consumers, or the community including and supporting the educational needs of all graduating high school seniors. A PKI model serving such broad communities is referred to as “open.” Open PKI's are still largely in the conceptual stages, and their difference from a network PKI may be viewed as a matter of degree. Conceptually, however, in an open PKI one entity or group of entities would provide the authority for the issuance of certificates that could be relied upon by a spectrum of different parties. The policy authority could be one organization, championing a particular approach on behalf of a larger community (GSA ACES model) or a collection of organizations developing a shared approach but willing to extend the PKI beyond their initial membership (ABA TrustID example). In these cases, the goal is to create a "portable Internet credential" that has broad utility for identifying oneself electronically -- beyond the originating community.

### 1.5 A PKI Model for Higher Education

The higher education community is an extraordinarily complex collection which comprises public and private educational enterprises; students; high schools; lending and other financial institutions; federal and state government agencies; employers; and other participants. Each of the models of PKI discussed above has a place in this arena.

The PKI Work Group reviewed a number of critical, frequently recurring and sensitive exchanges of information that occur among students, high schools, postsecondary institutions, guaranty agencies and employers. These involve the exchange of application information, test score data, grades, transcripts, and loan information. If these are to be successfully moved to a public-key based exchange, some type of open PKI will ultimately be necessary, as it will be impossible to fully characterize the participants in real time.

These transactions:
- Cut broadly across constituencies related to higher education, including schools, students, and potential employers
- Are often time-sensitive
- Require authentication and confidentiality

These transactions appear to fall primarily in the arena characterized by an open PKI.
The PESC PKI Work Group recognizes another important ongoing study of PKI issues in higher education – a PKI Work Group of NET@EDU, under the auspices of EDUCAUSE. The initiative supports X.509v3 digital credentials as the de facto standard for institutions. EDUCAUSE, the University Corporation for Advanced Internet Development, the Corporation for Research and Education Networking, and the Coalition for Networked Information endorsed these credentials in a March, 2000, letter to Federal agencies, encouraging use of the standards when dealing with higher education institutions.

1.6 Reference URLs:

For a more complete overview of how digital signatures work and how they are supported by a public key infrastructure, see the following references.

http://www.gits.gov
Access With Trust, the Government Information Technology Services (GITS) Board and OMB's description of how PKI can enable many of the goals laid out in the Access America initiatives.

http://www.rsasecurity.com/rsalabs/faq/
RSA Laboratories' Frequently Asked Questions About Today's Cryptography. This FAQ covers the technical mathematics of cryptography as well as export law and basic fundamentals of information security.

Digital Signature Trust's website containing useful links to get a demonstration certificate; view a live demonstration of the relationship between a certification authority, subscriber, repository and relying party.

http://www.pca.dfn.de/dfnpca/pki-links.html
The PKI Page, from Germany.

http://www.educause.edu/netatedu/groups/pki/report.pdf
A well-written explanation of PKI technology which appears on the NET@EDU as an output of its PKI Work Group.
Universities have special authentication and security requirements pertaining to their students that are quite different from a commercial or retail model. These derive from both the nomadic nature of the core community and also from the need for a portable certificate. Students use their student ID's very broadly and for a wide variety of campus-based services (building access, meals, library access), and may use a number of different computers across the campus and at home. Accordingly, the need for a portable certificate, located in a smart card or other token, plays a much greater role for this enterprise than it is likely to in an office- or home-based environment. An important exception is military bases, where there are very similar drivers.

Examples that will be discussed below include University of Texas and University of California.

### 2.1 The University of Texas System (U.T.) – Closed Model

The University of Texas System provides a good example of an enterprise-oriented or closed PKI in higher education. The University of Texas System Strategic Information Council approved the Phase I Implementation of the University of Texas System Public Key Infrastructure (UTSPKI). Implementation of Phase I began in January, 1999. The University of Texas System consists of 15 component institutions, including four-year undergraduate, graduate, health science centers and medical schools. The UTSPKI is designed to aid the System and the component institutions in accomplishing their missions by making the move into cyberspace much easier.

The University of Texas Health Science Center at Houston will use a "Locally Hosted Option" to issue and manage certificates. This process allows users listed in a University of Texas at Houston LDAP Directory (Lightweight Directory Access Protocol Directory) to apply for certificates from the CA. Once a user's identity has been appropriately verified by a local registration authority (LRA) at the University of Texas at Houston, his or her certificate will be issued.

The remaining 13 components and University of Texas System Administration will use a "Remote Hosting Option" in which users will directly request certificates from the CA. The web interface for requesting a certificate is customized for each University of Texas component CA. Local registration authorities (LRAs) at each of the components and at the System Administration will verify the identity of each individual requesting a certificate. Upon identity verification, the requesting user will be issued a certificate.

On March 25, 1999, a Master Service Agreement was signed with a commercial certificate authority, for a period of three years. Fifty thousand digital certificates were purchased. There was an allocation made to each institution and the University of Texas System Administration. Each institution was notified of their allocation and allowed to request more certificates. A final allocation was made, which completed the distribution of all 50,000 certificates. The University of Texas certificates issued to individuals are "High Assurance Certificates" as recommended by the University of Texas System Information Technology Management Council (4/9/1998) and approved by the Strategic Leadership Council (4/15/1998)

So far, items completed in Phase I include activation of a locally-hosted certificate authority at the University of Texas Houston, activation of a remotely-hosted certificate authority at the University of Texas System Administration, and a UTSPKI training session held on June 3, 1999. Also, a request was submitted on June 16, 1999 to the U.T. System Office for General Council for Opinions relating to UTSPKI usage. On August 17, 1999, a Report of the Digital Signature Task Force – U.T. System Office of General Council – was completed. It can be viewed at [www.utsystem.edu/ogc/intellectual property/digsigtf.htm](http://www.utsystem.edu/ogc/intellectual property/digsigtf.htm). Examples of online forms that can be signed using digital IDs were place on the web on August 21, 1999, at [www.uth.tmc.edu/xorgs/utspki/signing-forms.htm](http://www.uth.tmc.edu/xorgs/utspki/signing-forms.htm).

The University of Texas has a number of initiatives out of the Office of Information Technology and Distance Education. The overall goal of the University of Texas Information Technology Initiative project is to identify system-wide information technology strategies so that components can more effectively compete in the 21st
century. These strategies provide the opportunity to use information technologies to improve the way University of Texas components achieve their basic missions.

More information on the UTSPKI project may be found at: [http://www.uth.tmc.edu/xorgs/utspki/index.htm](http://www.uth.tmc.edu/xorgs/utspki/index.htm).

### 2.2 University of California (UC) – Closed Model

The University of California provides a second example of a closed, enterprise-based PKI. The initial pilot that began in March, 1999 included a locally developed Certificate Authority based on the Netscape CA server. This CA delivered certificates to applicants via a self-service web page interface. Identification was based on existing university systems that utilized userid and password. The CA was in the University of California Office of the President (UCOP) trust chain so that certificates could be used with UCOP applications. Authorization support was not expected to be part of the initial pilot -- applications would unpack the user identifier (UID) from certificates and use existing mechanisms to determine whether or not to grant access. They expected to select no more than 50 testers from a mix of students, faculty and staff. Four initial applications were used during the pilot including employee benefits and an internal staff website.

Authentication was possible in all applications either with certificates or with logonid and password. A general description of the architecture of the initial University Public Key Infrastructure implementation was forwarded to each of the ten campuses of the university. Additionally, each campus was advised of several decisions they needed to make in anticipation of the pilot getting underway this spring.

Initially, all functions will be run on a single platform located at the UCOP Data Center. Separate Certificate Authorities (CAs) will be run for each campus. The Registration function (RAs) will be performed over the network from each campus using standard Web browsers. Each CA will be identified appropriately in any certificates issued so that the CA function can moved to the campus at a later date, if desired.

At startup, the root Certificate Authority will sign a certificate for each of the campus CAs. For the initial rollout period, ten instances of the Certificate Authority (CA) and the Registration Authority (RA) -- one for each campus and UCOP-- will be run on the same server. Registrants or designated Certificate Registrars on each campus will be responsible for interacting with that campus’ RA over the network, as shown below:

```
ROOT CA
  (self signed)

UCB CA

UCD CA

UCI CA

UCSF CA

UCB RA

UCD RA

UCI RA

UCSF RA

UCB Registrants

UCD Registrants

UCI Registrants

UCSF Registrants

LDAP Directory
(all CAs)
```

Two means of initial authentication will be supported, each resulting in a different strength certificate. Using an automated method, authentication will be performed against data in the University Directory. A second,
“manual” process is also supported. Under this method, an individual visits a Certificate Registrar in person, who, after confirming the physical credentials of the applicant, uses a Web browser to access the RA and obtain a certificate for the applicant. The certificate is placed on a diskette and given to the applicant. The in-person method is the only means of authentication available for use by students.

Certificate information will be published to a lightweight directory access protocol (LDAP) directory devoted solely to this purpose. Again, initially the LDAP directory will be operated at UCOP. Some campuses may want to operate their own local RA or RA and CA. This capability will be supported at some time in the future.

Each location will support at least two roles: a Certificate Policy Administrator, and a Certificate Registrar. The Certificate Policy Administrator is responsible for specifying local certificate and enrollment page contents, managing reporting, and any location-specific configurations. Following the chain of certificates hierarchy, the person in the Certificate Policy Administrator role receives his/her authentication from the root Administrator at UCOP.

The Certificate Registrar performs local certificate management functions. These include manual approval and rejection, face-to-face (manual) authentication, revocation, and generally managing day-to-day certificate operations. In other installations, the Certificate Registrar’s role typically is performed by someone from the HR or Student Registrar areas (or one from each). The Certificate Registrar’s access privileges are granted by their local Certificate Policy Administrator and access at the workstation level is authenticated via smart card. The only client software necessary is a browser. There is nothing to preclude a campus having one person play both the Certificate Registrar and Certificate Policy Administrator roles, and some may find this advisable during the pilot. For more information, refer to the following URL: http://www.ais.ucla.edu/auth/index.htm.

2.3 Automotive Network eXchange (ANX) – Network Model

The Automotive Network eXchange (ANX®) is a secure and reliable global network infrastructure that replaces complex legacy networks and facilitates the re-engineering of supply chains within the automotive industry. The ANX, introduced by the Automotive Industry Action Group (AIAG) in 1995, was designed to improve on the inefficiencies, network inconsistencies and lack-of-data-security offered by the public internet. The ANX securely connects trading partners electronically – allowing them to collaborate on product design and development; solicit and process orders; facilitate just-in-time manufacturing, coordinate purchasing, and post shipping schedules. ANX provides a safe, robust and neutral trading environment for companies to communicate, collaborate and facilitate supplier relationships.

In March of 1998, the AIAG selected the first provider of certification authority services for the network, which is designed to meet the highest degree of security and privacy for data through using digital certificates.

ANX Service is separate and distinct from the public internet. ANX Service is delivered over a virtual private network established solely for the transmission of ANX Traffic. This virtual private network (VPN) is not shared with any other users. ANX Service uses the TCP/IP protocol for networking but uses facilities that at a minimum are logically separate from the facilities used by the public internet. The Trading Partner’s ANX Interface may carry traffic destined for both the public internet and the ANX Network.

The first internet protocol security (IPSec) certificate was issued in the ANX production environment in September 1998 by Digital Signature Trust (DST), ANX’s Root CA. Through its TrustSource Plus Certification Authority Service, DST issues certificates to ANX trading partners and manages all aspects of the certificate lifecycle. Parties seeking to rely on certificates tap the TrustExchange repository, the DST-managed database for ANX certificates, to check a certificate’s status. The repository enables trading partners to communicate over the ANX Network and feel assured about the identity of the sender and the privacy and integrity of their transactions.

2.4 The Digital Library Federation – Network Model
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. The DLF’s efforts in using PKI presume the need to rely upon certificates from multiple independent CA’s, so it is a more complex example of a networked approach. Broad success will hinge heavily upon surmounting both policy and technical interoperability barriers.

Under DLF auspices, the California Digital Library, Columbia University, JSTOR (Journal Storage, an on-line repository of scholarly journals), and OCLC (Online Computer Library Center) have developed a protocol that enables an information resource provider to verify that a user bearing a digital certificate has authority from a home institution to use a requested resource. The prototype system developed combines the use of X.509 digital certificates for authentication with a directory service providing authorization to licensed resources based on user attributes. An architecture statement has been developed as a result of the prototype development work as well as a project overview. It should be noted that at least one of the organizations mentioned above utilizes IP authentication for web access; this is a clear instance where use of digital certificates would improve service to users.

The group has also made the assumption that each institution will have its own certificate authority (CA). Thus, the information contained within the certificate is sufficient to identify the institution. Clearly, the architecture will need to address the case in which the institution is not also the CA, possibly by requiring that the institution be identified in a designated field within the certificate. Another assumption is that the full authentication and authorization process is performed infrequently (e.g., once per "session") so that directory load can be minimized.

One of the key design decisions made early in the design process was the separation of authentication and authorization requirements. Authentication for the transmissions, messages, and their originators required a different processing than that for authorization, which was to ensure that the user was authorized for access to the system, application, and its underlying data. The criteria of localization of information, accommodation of temporal change, and privacy considerations led to the conclusion that authorization information cannot be explicitly included in the certificate payload. Thus, the institution must have a directory or attribute server which, given some information from the certificate, can determine eligibility for the service. To simplify the directory and access protocol discovery, it was decided to place a URL encoding the query in one of the X.509 certificate attribute fields. The service provider does not need to interpret the contents of this URL beyond interpreting it as a URL.

For more information, please refer to the following URL: http://www.clir.org/diglib/

2.5 GSA ACES – Open Model

The U.S. General Services Administration (GSA) is sponsoring an initiative called Access Certificates for Electronic Services (ACES). Much of the impetus behind ACES flows from the Access America initiative championed by Vice President Al Gore. The primary goal of Access America is to leverage information technology to deliver comprehensive government services to Americans and to dramatically increase government productivity. In line with this goal, ACES is meant to facilitate the public’s access to government services via the Internet.

ACES is intended to enable individuals and businesses to efficiently conduct business with the government electronically via the use of digital signature technology. Government agencies, individuals, and individuals acting on behalf of businesses may receive digital certificates that positively identify them online. ACES certificates will enable agencies to authenticate users prior to granting access to confidential, personalized information. Users gain assurance that their identity will be validated before personal information is released, and that the information has not been tampered with in transit.
As a result, government agencies will be able to provide more personalized services online, accept various kinds of document filings online, and make accessing federal government services faster and more convenient. A citizen who gets an ACES certificate can use that same certificate to interact with any federal agency participating in the ACES program, an example of the “open model” PKI. In this case GSA has provided a policy authority on behalf of the Federal government. GSA created a certificate policy designed to meet the needs of the largest possible number of Federal agencies needing authenticated communications with their constituents. In addition, GSA developed, or sponsored the development of, the needed supporting contractual documents, including contracts with each of the three ACES vendors; the vendors’ certification practice statements, which support the CP; qualified relying party agreements entered into by participating agencies, and subscriber agreements for participating citizens and businesses wishing to use an ACES certificate. This constitutes a broadly open Federal-purpose PKI that agencies may opt into as they become prepared and have a need.

2.6 ABA TrustID® Program – Open Model

The banking industry has also stepped up to sponsor the creation of a trusted online identity credential based on public key cryptography, analogous to an ACES certificate but with a broader goal. Where ACES is intended for Federal purposes only, the bank-sponsored credential, called a TrustID certificate, is designed to be broadly acceptable across the Internet economy. Banks will issue TrustID digital certificates to business and consumer customers to support the projected large volume of business-to-business (B2B) and business-to-consumer (B2C) e-commerce.

The American Bankers Association (ABA) is sponsoring this online trust initiative and is hosting a central repository for all bank-issued credentials that is backed by a set of governing policies it manages. In this way, the ABA is adapting its traditional role of providing trust to the needs of businesses and individuals on the Internet.

In addition to its more traditional role, the ABA is dedicated to facilitating electronic commerce by creating a secure environment for financial institutions and their customers. The TrustID certificates that ABA-member banks will issue to customers are designed to bring “portable trust” to Internet e-commerce in the same way that the addition of the Visa brand changed a local bankcard into a trusted, international payment tool. Where the Visa brand promised a “guarantee of Payment,” the TrustID branded certificate promises a "guarantee of identity."

This initiative represents the broadest example of an open PKI in that TrustID certificates are explicitly intended for broad use across the economy. Organizations wishing to rely on TrustID certificates do not have to be part of the existing banking community or be one of the founding organizations, but have only to enter into a relying party agreement under the TrustID Certificate Policy.

For more information, refer to the following URL: http://www.digsigtrust.com/fs.html.
3 Issues in Deploying and Using Public Key Technology in Higher Education

3.1 Acceptance by Consumers

The public at large, and students in particular, have shown great willingness to use the Internet and other electronic means to transact business. Hesitancy to shift from traditional to electronic services typically centers around four arenas: access to the technology; ease of use; access to technical support; and, increasingly, trust. Since trust also addresses areas of privacy and confidentiality, it will be further discussed in section 3.2.

Access to the technology

Access to the Internet is probably not an issue for most schools, postsecondary institutions, employers, and other institutional participants, since most of the services of a PKI are or will become available from any current browser. While probably anyone who wants it can get access to the Internet through their school or a public library, delivering and using certificates on a publicly shared computer still presents a lot of customer service support challenges. The customer service aspect may be mitigated by the use of smart cards, but smart cards require a substantial investment in hardware and software.

Ease of use

Most of the desired security services are available using standard Microsoft or Netscape browsers and email clients. Those services not readily available can typically be achieved using plug-ins, and there is an expectation that as markets develop for these, the major browsers will incorporate them. However, requesting, downloading, protecting and managing a certificate will be fundamentally new tasks for most people, and many may hesitate to commit to converting a business transaction from something known to something completely unfamiliar. Adoption rates may be expected to be fastest among communities that practice some form of electronic data interchange (EDI), have already been exposed to certificates in another context, or among students who are less committed to how things have been done in the past.

Technical Support

In light of the ease of use issues, technical support will be critical to the success of any PKI. Further, since Microsoft and Netscape manage certificates very differently (and Microsoft IE handles certs differently from one browser version to the next), tech support offerings will have to be quite sophisticated.

3.2 Trust

Notwithstanding the public’s willingness to adopt electronic business practices, there is an expectation that electronic transactions should have, and should be perceived to have, a measure of security that is as good or better than that provided by the prior paper-based system. In the white paper, “Why is Certification Harder Than It Looks?,” by Ed Gerck (http://www.mcg.org.br/whycert.html), Mr. Gerck attests that a secure design is not the same as having trust in the protocol, trust in the correctness of the PKI model, and trust in the effectiveness of PKI. Two basic areas of trust, privacy and confidentiality, are very large concerns for the general public.

Confidentiality

Confidentiality is the protection of transmitted data from passive attacks, such as unauthorized monitoring of the application or its data or transference of the data over the network, and the protection of network traffic flow from analysis. This requires that the information in the computer system and information that is transmitted is accessible only by authorized parties and the information is not disclosed or revealed to unauthorized persons. Therefore, it is incumbent on the CA and the application providers to assure that the applications are safe, that the use of certificates will provide strong authentication of the participants, that transactions cannot be intercepted, altered, or viewed in transit, that the data collected is held in a safe
environment, and that there are sufficient means available to the certificate subscribers to protect their own keys.

**Privacy**

Privacy is a concern that has to do with the use of the information gathered in support of the issuance of certificates, and in the applications themselves. This nation has a deep, long-standing commitment to the concept of personal privacy, and so anything that looks like a “national identifier” is suspect. So, too, is the notion that information collected for identification and authentication purposes might be sold on the commercial market. It will be incumbent upon CAs, and similarly upon education and governmental applications that collect personal information, to communicate very clearly that they are in the trust business and not in the information business.

Business communications which are sent over traditional means, US Mail or proprietary networks, are protected by laws as they travel from sender to receiver. However, business communications that travel over public networks such as, the Internet, are not protected by federal or state law. Organizations that use the public network to transmit business communications must ensure they take the necessary steps to satisfy their customers concerns for data integrity and confidentiality.

### 3.3 Interoperability

Interoperability is a concern when using any technology including PKI. The major areas of concern for interoperability are with the various standards, the actual technology, and the policies created to support the PKI. Also, note that initiatives and pilots are currently addressing these challenges. Each of these is discussed in the following paragraphs.

**Standards**

There are many groups involved with standards creation and promulgation for PKI. Some of the groups that are working on formal standards in these areas are the International Standards Organization (ISO) X.500, the Internet Engineering Task Force (IETF) working groups, and the American National Standards Institute (ANSI) X9. A set of standards put forth by RSA Laboratories dubbed the Public Key Cryptography Standards (PKCS) serve as de facto standards within the cryptographic and PKI communities. The National Institute of Standards and Technology (NIST) also maintains a number of cryptographic standards, called Federal Information Processing Standards (FIPS) and coordinates validation programs for many of these standards. Other relevant efforts include the Federal PKI (FPKI) Steering Committee, the Department of Defense PKI. Standards have also begun to mature for three of the application areas with the broadest initial impact: secure email, secure web access and secure remote dial-in. However it is important to recognize that the existence of a standard, and even compliance with those standards, is a necessary but not sufficient condition for interoperability.

**Technical interoperability**

Despite the fact that we have a standard in the form of X.509 v3 certificates, certificates issued by one CA are not routinely recognized by another. The standards offer a great deal of flexibility in how they are implemented. Interoperability is achievable but requires commitment and investment on the part of all participants.

**Policy interoperability**

A critical premise of the NACHA study below is the primacy of policy considerations over technical ones. The NACHA team addressed technical and policy issues simultaneously, but concluded that the creation of a policy authority should have been the first step, and that a policy authority and its products (certificate
policy) are foundational to the ability to interoperate at a later time. This is the approach that ANX took in establishing its PKI.

**Other Interoperability initiatives: Bridge CA and NACHA**

Two other PKI initiatives and pilots have also been underway to support interoperability between technology and vendors.

**Federal Bridge CA**

The Federal PKI Policy Authority facilitates interoperability through the Federal Bridge Certificate Authority (FBCA). The FBCA focus is to determine the certificate policy mappings between various governmental CAs. The project is established such that all agencies that interoperate through FBCA are voting members for the project. Interoperability of the CA’s through the FBCA is not a requirement, but it an attractive goal.

In order for this project to succeed some boundaries had to be established. The first set of boundary conditions is with respect to the technology. The second boundary conditions were policy and political boundaries.

The technology boundaries are based upon standards. The first of these is compliance with FIPS 140-1, 186. This required a level 3 crypto module for FBCA. Another standard base was to meet the MISPC to maximum extent practical. The final standard base was compliance with X.509v3 certificates. This included the mapping the certificate policy of these certificates as a method of ensuring the success of FBCA. One last technological requirement was the use of commercially available software and hardware.

The political and policy boundaries were based upon a desire for a solution, which was as fully “inclusive” for vendors as possible, meaning that this was not a “single or sole” source CA solution. The FBCA has to support four levels of assurance: rudimentary, basic, medium, and high. The certificate policy generated for the mappings is analogous to the certificate policy (CP) used in Canada. Again, it is important to note that interoperation between the various CA’s is not a mandatory goal or requirement of the FBCA.

**National Automated Clearing House Association – NACHA**

According to the results of the Certification Authority Interoperability Pilot conducted by the Internet Council of NACHA - The Electronic Payments Association, banks can serve a value-added role in electronic commerce by acting as certification authorities on behalf of their customers. The results of the five-month pilot are documented in a NACHA publication, *Certification Authority Interoperability: From Concept to Reality*, available at [http://www.nacha.org](http://www.nacha.org).

**3.4 Key Storage**

Key storage is a particular problem in the higher education environment which includes students who are mobile and may use numerous computers for various transactions. Machine-specific solutions for key storage are not practicable in such an environment. It has been suggested that directory storage of private keys is an option, although trust in the security of such a directory is required.

The appearance of smart card readers on major brands of laptop and desktop PC heralds a new era for authentication at the desktop, suggesting that smart cards may be the answer for a mobile population. Several major PC manufactures are beginning to incorporate this technology into their products.

The smart card industry still faces issues of standards compliance, and other thorny issues relating to PKI. For instance, keys generated on a crypto smart card cannot be backed up by the PKI -- the card simply will not allow the keys to be exported since it would violate the premise of non-repudiation. However, it introduces an important single point of failure -- if users lose their smart cards they lose their private keys and their digital identity.
3.5 Certification Authority Services

The UT Austin and University of California examples above illustrate two models for obtaining certificate authority services. As an institution determines its role in a developing PKI and what services should be outsourced, certain areas deserve careful scrutiny. Some areas to be addressed are the knowledge of the technology and its implementations, the policies and procedures under which the certificate authority will operate, the data processing requirements of the certificate authority, including the hours of operation, repository needs, and key recovery implications as well as the facility of the certificate authority, the amount of risk and liability to be borne by the certificate authority, the applications to be supported by the PKI and the underlying use of the certificates, and customer support concerns. Each of these areas are discussed in the following sections.

Technology Knowledge and Implementations

Underlying knowledge of the technology and its implementations are paramount to understanding the use of digital certificates. Currently, there is no one standard for what a certificate means or for what is to be used or for how it is to be used. It is incumbent upon the operators of the PKI and the certificate services to understand how digital certificates will be used within the educational institution and with its partners. Will they be used for authenticating users to an application or to a system? Will they be used to allow servers to authenticate to each other? Will they be used for digitally signing student documents, such as thesis submissions and term papers from students to faculty, or strictly for administrative purposes? Will they be used for encryption? Is there a need to have different levels or classes of certificates? All of these questions and more play an important part in the knowledge of how the technology works and where the technology can be implemented.

Policies and Procedures

Defining policies and procedures are critical steps in using PKI. If digital certificates are used as a means for projecting legal assurances that security risks are controlled, then the scope of these policies and procedures incorporates every security issue. Every common practice, usage, convention, and risk factor must be addressed if these policies and procedures are to be enforced without loopholes. If just one exploitable loophole exists, the integrity of the CA and the infrastructure, which it supports, will be undermined. The vast majority of overt policy and procedure violations typically are borne because of unsecured assets, in this instance the certificate authority, or complacent monitoring and enforcement of these policies and procedures. Violations usually occur from exploiting weaknesses in these policies and procedures. Accordingly, an essential component of policies and procedures is the audit provision that ensures adherence.

Data Processing and Facility Requirements

Within the realm of the CA, the data processing and facility requirements must work in conjunction with other security measures, including, but not limited to, physical security, personnel security, administrative security, and media security.

Physical security is the use of locks, doors, other physical controls, and tamper proofing of sensitive equipment. Measures are taken to secure the facility in which the CA will be housed. Various questions must be asked and answered that will define the physical controls and, thus, the security, of the facility. Access controls protect against unauthorized access to any resource, including the facility. Unauthorized access refers to use, disclosure, modification, destruction, or issuing commands that are not in accordance with identified policies and procedures. In some instances, the use of guards, monitoring devices, locks, and access control devices, such as keys, tokens, and biometric measurement devices are used to secure the facility as well as lead protected walls and ceiling and floor breaks.
Personnel security is the process of screening employees to work in the secure CA facility. Personnel must identify with the sensitivity of the position, be trained to understand and comprehend the security issues related to the task and position, and attend the proper awareness programs. Additional personnel security and controls include the use of background checks, training and retraining, job rotation, sanctions in the event of unauthorized actions, bonding of personnel, monitoring personnel, auditing personnel, and special contractual provisions. The CA has obligations to investigate and oversee personnel who are in trusted positions and to remove them in accordance to the documented policies and procedures if the circumstances warrant. For institutions heavily reliant on student labor pools for information services support, these security targets may be unattainable internally.

Administrative security of the facility includes, but is not limited to, controlling the import of software to the system and within the facility, investigating security breaches to the facility, reviewing audit trails and records, and reviewing the accountability of controls.

Media security for the security includes, but is not limited to, controlling the marking and reproduction of sensitive stored information, ensuring that discarded paper or magnetic media containing sensitive information are destroyed securely, and obtaining proper procedures for secure backup and off-site storage in another secure facility.

Data processing requirements identify how certificates are processed through the CA. These include, but are not limited to, hours of operation, data backups, off-site storage, emergency procedures, and job scheduling. While similar to many other management information systems, these data processing requirements must also include security factors with respect to the physical storage of backup media.

**Risk and Liability**

The manner in which a CA warranties its services and apportions its liabilities will impact the perception of trust by the CA. In other words, how well a CA guarantees services and determines its liabilities will be perceived by its users that the CA is trustworthy. The CA must be solvent. The CA must have sufficient financial resources to maintain operations and perform its duties in the present as well as in the future. The CA must be reasonably able to bear the risk of liability to users and subscribers. The CA should demonstrate sufficient resources, including insurance, in order to provide reasonable financial responsibility when acting as the trusted third party.

**Applications Supported**

The complexity of security requirements in modern application protocols have forced a trend toward use of application security measures. In a messaging application, secure messaging demands writer-to-reader protection in an environment in which messages may traverse multiple network connections and may be stored and forwarded through unknown application-level gateway systems. In a web application, two areas of concern exist. The first concern is the compromise of the web server and the second is the compromise of user communications. Both of these web problems need to be addressed through standard application security protocols supported by the web server and browser products that are available from many commercial vendors.

“Home grown” or customized applications that need to have security incorporated into them must be maintained and have a method for recognizing user certificates, validating the user via the certificate and potentially have a need for backward compatibility to recognize expired certificates. Additionally, these applications tend to have a need to be able to communicate with each other – oftentimes between campuses, between client servers, and between clients. It is important to address this during the early stages of PKI planning.
**Customer Support**

Customer and helpdesk support will need to be available, especially for a new system. Hours when customer support is available must be determined based upon when the application is used. Training on the application must be provided to the people who are answering calls to the helpdesk. An application, such as Remedy, should be used to track the number of calls, the type of calls, and how the call was resolved. People who work on the helpdesk must be appropriately screened for tact and diplomacy, especially when dealing with frustrated users.

User documentation for the application will need to be generated and distributed. Ideally, the design of the application will allow that its use will be intuitive to the user. However, in some cases, written documentation for using the CA and its supporting applications will need to be written, tested, published, and maintained over the lifetime of the CA and supporting applications.

**Cost of PKI**

The table below compares costs of an organization providing its own certificate services and costs of outsourcing certificate services.

<table>
<thead>
<tr>
<th></th>
<th>Infrastructure</th>
<th>Liability</th>
<th>Policy Development</th>
<th>Directories</th>
<th>Updating Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-House</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Outsource</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Previously mentioned considerations of technology and its implementations, policies and practices, data processing, risk and liability, application support and customer support can be very cost prohibitive for the normal institution. Not only must these costs be borne initially but they are recurring in terms of recurring personnel training, enforcement of the policies and procedures, and helpdesk support. Additionally, many institutions are not equipped to handle the potential damage to their reputations if a lapse in security occurs, private keys are made available publicly, or other infraction of the policies and procedures occur.

While the preceding paragraphs address the implementation concerns of managing certification services in-house, the primary questions an organization must answer and address are:

1. How much verification is necessary? Is the real need to identify a person or organization, or a relationship between the educational institution and the certificate holder?
2. Does the educational institution need control over the issuance and the revocation of the certificate?
3. Does the educational institution want to manage the process and the implementation internally?

With the emergence and widespread use of new technologies, such as PKI, it is important that individuals be able to use a given digital signature within multiple settings and avoid the need for different digital signatures for different groups. Higher education institutions, for example, might want digital signatures that can be recognized and used within the institution’s various offices; with state higher education offices; with other institutions; with a variety of Federal agencies providing student, research, and institutional support; with professional associations; and with business, legal, and financial institutions.

Today, there is neither one technology nor one standard. Various organizations, such as the Federal government, are working to achieve these goals for their own business needs, as exemplified by the General Services Administration’s ACES contract.

Thus, it is important to promote standards and interoperability and consider carefully before embarking on an approach that may not be sufficiently flexible to achieve these goals. Higher education institutions can either create their own certificate services or use commercial services. To the extent that the latter may already have addressed standards and interoperability – and considered the implications of evolving technology – it may be advisable for institutions to reach the goals of interoperability by outsourcing certificate services.
4 Workgroup Recommendations

The PKI Work Group recommends that PESC formally support and promote the use of PKI for promoting secure electronic commerce in higher education. This would include:

- Posting a statement of support for PKI on the PESC web site and a discussion of the importance of standards in the use of PKI;
- Dedicating an area of the PESC web site for information and materials on PKI and its use in higher education;
- Tracking digital signature legislation in Congress and at the state level;
- Providing support for and cooperating with initiatives to employ PKI technology in higher education.
- Recommending transactions that would be ideal candidates for PKI.

There are a number of organizations within the postsecondary community that have an interest in working toward the consistent use of PKI in higher education. The focus of these organizations varies. Some, such as the Corporation for Research and Educational Networking (CREN), are interested in providing interoperability among university enterprises by providing a common root. Others, focused on subsets of the university business enterprise and their business partners, are centered around functional areas such as financial aid or research grant management.

The Work Group, recognizing the unique position of PESC with its enterprise-wide membership, suggests that its primary role in this issue should be to promote appropriate uses of PKI. To do so, PESC should serve as a monitor of PKI activities in higher education and a conduit for sharing information on these activities. An example might be to follow the institutional and Federal acceptance of X.509v3 digital credentials and make that level of acceptance known to the higher education community. In this way, PESC might facilitate ideas that lead to demonstrations that could develop into larger efforts to create a PKI. PESC might thus bring together various parties who could work together on PKI applications in areas of mutual interest.

Through its study of PKI for higher education and its potential for use in the higher education community, the Work Group recognized that this paper naturally raises a number of unanswered questions. For example, what opportunities exist for PESC investment and/or involvement in a network or open PKI for higher education and what are the likely returns for the membership? What assumptions and hypotheses are associated with PKI that need to be validated, tested, or researched? What are the gaps in the infrastructure that PESC members should be aware of or actively engaged in resolving? What gaps in our knowledge need to be researched and articulated? Are there specific practices that PESC should recommend to its members?

To accomplish the needed promotional, tracking, technical and information-sharing activities, the Work Group proposes that PESC establish a standing committee and contract with a PKI expert to continually survey PKI activities in the higher education community and make that information available to members through published articles, web links, and other electronic communication. With this support, the Work Group believes that PESC can truly further the use of PKI in higher education.