

**Why PKI:
The Need for Strong Crypto-Technology in the University**
David L. Wasley
University of California
October, 2001

Note: This memo was written to articulate the range of university applications for which strong digital cryptography should be available.

The Information Technology (IT) infrastructure of the university has become not only integral to the operation of the institution but mission critical in its overall impact should its reliability be compromised. One of the weaker aspects of that infrastructure has been the lack of reliable and generalized support for strong digital credentials and other uses of cryptography to ensure secure and auditable operation of critical institutional activities. This briefing paper identifies a number of areas in which Public Key Infrastructure (PKI) technology could play an important role by providing those functions.

Public Key cryptography¹ provides a sophisticated yet fairly straight forward way to achieve a number of important functions, including:

- highly reliable digital credentials supporting authentication and leading to scalable and flexible authorization;
- strong encryption supporting data security in transit and storage;
- true digital signatures supporting auditable transaction validation;
- document integrity through the use of digital signature mechanisms.

PKI digital credentials

Secure and reliable authentication of individuals and other entities in the IT environment is the basis for managing access to resources and granting privileges. Digital credentials can form the cornerstone of a secure and reliable IT environment by providing that function. To explain this it is essential to define what digital credentials assert before describing how they can be used in any particular context.

A PKI digital credential, usually referred to as a PKI certificate², does not establish “identity” in the general sense of the word. Identity is really the collection of attributes, roles, privileges, and associations that an individual has with respect to the rest of the world. Identity can be specific to an individual, such as a Social Security number, or apply to a class of individuals, for example

¹ Public Key cryptography refers to the use of asymmetric algorithms and a pair of crypto keys. If one of the keys is used for encryption, only the other one can be used to decrypt that encrypted object. Typically one key is closely guarded by the owner but the other key can be made freely available, hence the term “public key” in describing this technology.

² The format of a PKI certificate is defined in the ISO x.509 standard. It includes reference to the certificate issuer, the certificate subject, and additional information to assist in confirming the validity of the certificate.

“student at UC Berkeley”. In some cases it may simply be ‘serial identity’ - an association with a prior appearance. For example, in completing an on-line application for admission, it might be important only that the person submitting material is “the same individual who began the application process last week.” Clearly the meaning of “identity” is context and application sensitive and thus a useful credential must be able to serve to establish appropriate forms identity in a number of different contexts.

The basic digital credential might contain some useful aspects of a subject’s identity but its fundamental value is in that it binds a digital token to a known physical entity. That token, which might be very complex or quite simple, then can be used in access control decisions. It could also be used to retrieve from a database additional attributes or privileges of the holder. It is this generalization of identity that leads to the considerable power and flexibility of the digital credential mechanism.

Digital signatures

An individual’s signature on a document is intended to convey some relationship between the specific individual and the logical content of the document. It might be an assertion that the content is valid or that the signer agrees with the stated content. In any case, it is the association of the content with the individual’s uniquely identifying mark that gives meaning to the signature.

It is possible to create a similar association with purely digital documents, using PKI technology. Having created that association, using the crypto-key known only to the holder of a digital credential, any change to the original document inherently will invalidate the signature. Therefore, if the signature does pass the validation tests, the document must be what the credential holder signed and only that particular known individual could have signed it.

Digital signature technology can be used to ensure the integrity of documents whether or not the association with the signer is important. The signer might serve merely as a trusted notary attesting to the document’s state at a given point in time. For example, a web site with important information relating to the institution could be “signed” in a way that a reader could tell whether it had been modified after signing. Similarly digital archives could be maintained in such a way that the occurrence of any modification of an archived document could be detectable.

Applications of PKI

The use of PKI technology to create and validate strong digital credentials, data encryption, and non-repudiable digital signatures can be of great value across the spectrum of activities supported by the university. Some applications that do or will require strong authentication, authorization, and data security and integrity include:

1) Access to licensed or otherwise restricted content

In order to fulfill the university's obligation to contracting parties, individuals who are granted access must be adequately identified as being qualified under the terms of the contract. Current mechanisms are extremely weak and often don't work if the User is off-campus.

New areas where both authentication and authorization will be important include access to university enterprise directories, data warehouses and records. Directories will contain some potentially sensitive and/or restricted data which must be made available only to authorized individuals. Business applications that need access to sensitive data also should be authenticated so that their authorization can be determined.

Software availability and support may be provided by external service providers. Access to these services, including the downloading of software and updates, must be restricted to individuals who are eligible under the terms of the service provider contract.

Eventually on-line instruction may be offered that will require authentication and authorization of its students. Papers and other class work may need to be digitally signed for submission to the instructor. Distributed on-line instruction may require that a single digital credential be recognized by multiple universities.

2) Student and Employee "Self Service" applications

Increasingly we are turning to individuals to retrieve their personal information themselves and/or maintain such information through web interfaces rather than paper forms. Access to personal information must be managed so that only the individual subject or qualified university staff can view and/or modify such data. In some cases audit logs must be maintained that reliably indicate the individual who performed a retrieval or modification. In highly sensitive cases it may be necessary to require a digital signature in order to conclude a transaction.

3) Auditable electronic transactions within the University

The university must use the IT infrastructure to streamline and distribute responsibility for a myriad of internal actions, such as hiring approvals, purchasing requests, payment approvals, personnel actions, student record submittals, etc. Some of these actions should be encrypted for data security. Most of these transactions should be digitally signed in order to produce an auditable record of their validity.

Furthermore, by combining roles and rules based authorization with automated workflow support, business processes within the university could become more efficient and distributed. Clearly the association of roles with specific credentials must be managed carefully and audit logs must be

maintained to enable post-transaction verification. However, the payoff in the long run due to simplified management and increased accountability likely will be great.

4) Electronic commercial transactions with external partners

Where "commerce" is loosely defined as "the exchange of objects of value", the risks associated with that exchange must be mitigated. Commercial transactions effected over the network may occur with a large variety of partners and may cover a wide range of financial values. Strong digital credentials that result in appropriate validation of responsibility are essential to make this activity scalable as well as auditable.

The university's digital credentials not only must be recognized by external partners but they also must lead to valid discovery of the holders privileges. For example, a purchasing agent might be eligible to submit a purchase order for up to \$20,000 without a second signature but may be required to get a countersignature for any transaction of a higher value. Digitally signed purchase orders can form the basis for secure and reliable e-commerce infrastructures with a broad range of commercial partners.

5) Data security

It is critical that sensitive information be protected against inappropriate interception while in transit across networks and/or retrieval when in storage. Today encrypted data transmission is used widely across the internet to protect data in transit. Asymmetric encryption ensures that only the intended recipient can decrypt and view the data.

Exchange of student or medical records (see below) is one area where this protection is required. Other areas include employee data and evaluations, research data, and university strategic plans. In applications where university business documents are encrypted, it may be critical in order to ensure business continuity that the decryption keys be escrowed in a secure manner.

6) Exchange of student or other sensitive records among institutions

The university both accepts student transcripts from other schools and provides transcripts to other schools. Such document must be signed by an authorized official and protected in transit from inappropriate interception. PKI technology can accomplish both.

Furthermore, the FERPA and HIPAA regulations require that certain records be made available only to specific eligible role holders, either within the institution or at other institutions. Digital credentials could be used to verify the roles of any individual to whom such information is being released.

7) Student loan application and management

Fifteen million or more students have loans backed by the Federal government through the Department of Education. The application for and management of these loans requires authentication of the student to the university, the Department of Education, and the eventual lender(s). Management of the loan requires that the student authenticate to the lender regardless of which university s/he is currently associated with. This 'serial identity' could be established through use of the university digital credential as an initial identifier, from which a loan-specific credential is generated for the particular student.

8) Grant applications and administration

Universities submit many hundreds of grant requests to many dozens of funding agencies. Today these are on paper with multiple copies and multiple signatures. This entire process could be transacted digitally and the resulting information captured to a database upon entry without recoding. Furthermore, once funded, the grant could be administered electronically by the research office and/or the principle investigator using their digital credentials for access.

9) Integrity of on-line content, systems, and software

signed software, web pages

Today a huge amount of information is available over the network but there is essentially no assurance that the information a reader sees is what was originally made available. Digitally signing on-line documents can allow readers to validate the integrity of those documents.

Similarly, software that is downloaded and even software and configuration files on critical systems can be digitally signed to ensure integrity. Several commercial software vendors are already doing this.

10) Information requests

In general, the university supports "public information" which is available to anyone but may also be asked for information that is only available to qualified entities. Such information may be in directories, databases, documents, or reports. Requests for information or documents made electronically and validated with strong digital credentials enable the university to observe appropriate policy with respect to information release. For example, requests for student transcripts should come from an entity that is qualified to receive them. Requests for Verification of Employment should be signed (or countersigned) by the employee in question. The reliable identification of the requesting entities can be achieved with digital credentials.

11) Access to IT-based services

Lest we forget, access to administrative information processing systems and services must be managed appropriately. Today this is done most commonly with individual IDs and passwords. A PKI-based credential system would enable a “single sign on” method for all campus systems. The use of roles and rules based authorization in conjunction with digital credentials for authorization would allow very simple and scalable management of access privileges.

New and costly IT resources such as distributed computing (e.g. GRID), virtual laboratories and distributed visualization systems will require strong and flexible access management systems.

The network itself is a resource that will offer differentiated services. Access to advanced network services such as multicast, higher quality of data transmission, and access to very high capacity research networks will need to be managed appropriately because there will be a differential cost for the use of these services.

12) Management of IT infrastructure

For many years PKI credentials have been used to establish secure data transmission between ‘web-based’ systems. For example, a server offering items for sale can ask the remote buyer for credit card information. The buyer’s computer first makes sure that the server is identified properly in a trusted digital credential and only then does it set up the secure data transmission.

Management of the IT infrastructure itself - operating systems and platforms, email relays, network active components such as routers and DNS servers, monitoring and activity logging systems - must be very carefully controlled since its availability and integrity is fundamental to the operation of the university. Strong digital credentials and the use of roles and rules based authorization can help ensure this.

13) Resource accounting

As the use of IT broadens, so too does the cost of operating and maintaining it. It is appropriate that the university be able to determine how such resources are being used, and by whom. Digital credentials can help enable resource use accounting so that appropriate management views can be developed. Resource use can be summarized by individual, by department, etc., based on the attributes associated with campus credentials.

14) Alumni access to post-graduation resources

Many campuses would like to maintain contact with and offer services to alumni. Issuing new credentials to alumni would be a daunting task.

Allowing the continued use of a digital credential system would be relatively simple and would bring with it the benefit of the stored knowledge of the individual's prior association with the university.

15) Digital records: notary, retention and archive

The university must keep certain records for defined periods of time, or sometimes indefinitely. Today many original records are in digital form, for example electronic memos, documents, or transaction records. There must be an appropriate way to archive and retrieve such records without resorting to printing them and filing the paper copy. The use of PKI digital signatures can enable a robust digital archiving system. Not only can the integrity of such records be ensured but the records can be searched and retrieved easily since they remain in digital form.

In some applications, it is important merely to verify the state of a certain document at a certain time. For example, laboratory notes or patient care records. PKI can be used to establish a 'digital notary' service that can sign such documents and include a data and time indication. Establishing this service as a trustworthy and authoritative service will require strong digital credentials and the use of strong data encryption technology.

This is by no means an exhaustive list of application areas. There also is a great deal of overlap among these areas. The intent of this presentation is to illustrate the broad range of applications for PKI within the university in support of the secure, robust, and reliable operation of the institution.

Comments to: david.wasley@ucop.edu