Mariana Podestá, Christoph Meinel:
Integration of a Public Key Infrastructure in a Virtual University
in Proceedings of the Argentine Congress on Computer Sciences (CACIC 2000), Ushuaia, Argentinien, pp. 1-8, 10, 2000.

Integration of a Public Key Infrastructure in a Virtual University

Mariana Podestá
Christoph Meinel
E-mail: {podesta|meinel}@ti.fhg.de
Institut für Telematik, Bahnhofstr 30 –32, 54292 Trier, Germany
Fax number: +49 (0)651-97551-12
Telephone number: +49 (0)651-97551-0

Abstract

Users in a virtual university normally gain access to the virtual campus and its resources using a valid username and password. Each resource may have a different passphrase that the user has to remember. Information transferred inside the virtual campus is sent in clear. Usually the virtual university does not provide a way of sending private data safely over the network. It is neither possible to determine the authorship of documents nor when they were written.
The model that we propose for solving these problems is based in the use of a Public Key Infrastructure (PKI) and digital certificates. These certificates are used for authenticating to the virtual campus using a single sign-on solution, for encrypting and/or signing data and for timestamping documents.
This paper shows the different components of a PKI inside a virtual university and explains the use of the certificates within it.

Key words

Public Key Infrastructure, PKI, digital certificates, virtual university, authentication, digital signatures, timestamp, Educational Computer Sciences

1. Introduction

A virtual university is based on the use of distance education methods through the world wide web [1,2]. In this way students in different places can study there and obtain the corresponding certification.

The main element of a virtual university is the virtual campus. Normally the student logs in using username and password, and may perform a series of activities:

1. read lessons and bibliography on each subject
2. send and receive information to or from the teachers, other students, the administration of the university, etc.
3. participate in chats, newsgroups
4. write and send partial examinations and exercises, and
5. have access to books, exercises, information about the different subjects and any other education material

Final examinations must be attained personally, because it is not possible (yet) to determine the authorship of the student.

Virtual universities provide all the information on confidence basis. Users just have to give username and password in order to use the virtual campus. Sometimes a passphrase is also needed to access the different resources inside the domain, i. e., users have to remember several passwords. Another point to stress is the poor security that the use of passwords give in this case. If the passphrase gets compromised, another person could access the virtual campus and its components and impersonate the user. The user himself has little or no privacy inside the campus. E-mails and documents are sent in clear and there is neither the possibility of determining the authorship of them nor the time when they were created. Exchanging private data with the university's administration could only be done by mail, fax or telephone. Therefore, there is a need of

- *confidentiality*: which provides privacy in the messages using encryption techniques;
- *authentication*: which determines the origin of a message and provides some kind of assurance that it has not been sent by an intruder in the name of the sender;
- *integrity*: the message sent is the same as the data received, i. e., the information has not been altered during the communication;
- *non - repudiation*: means that a sender can not deny later on the authorship of the message sent.

All these properties are offered by a Public Key Infrastructure (PKI). [3, 4]

A PKI is a complex organisation which uses public key cryptography and digital certificates to achieve security in communications. A PKI is based on public-key cryptography [5] and this kind of cryptography states that each entity in a communication has a pair of keys : a public and a private one. Any data encrypted with a public key can only be decrypted by using the corresponding private key. The public key is publicly available while the private one is only known by the entity to which the pair of keys belongs. To be sure that a certain key pair really belongs only to one person it's necessary to use some kind of "document" which binds a public key to a specific person. Such a document is called a "digital certificate". When a certificate is generated, it will be installed in the browser of the user. The private key is stored in a database, which is (normally) located on the user's hard disk. The user must remember only one password: the one that protects this database.

In a virtual university, digital certificates could be used for:

- authentication to each resource of the virtual campus and to the virtual campus itself
- digital signatures of documents
- encryption of data
- timestamping files

Now that we have explained the properties of a PKI, we can redefine the activities, an user can do in a PKI-based virtual university. For example:
Exchange of information with other persons needs:
- confidentiality: only the intended receivers should be able to read the information and
- authentication: to know that the information really came from the sender.

Sending exercises per e-mail needs:
- non-repudiation: to have the authorship of the user,
- authentication and
- integrity: the exercises were not altered during the communication.

This paper describes a model of the possible use of a PKI inside a virtual university. We will explain the different components of it: policies, services and professionals. At the end we will describe the use of certificates and the benefits that are obtained of its use inside a virtual university.

2. Use of a PKI in a virtual university

We propose the definition of an internal Certificate Authority (CA), to issue, manage, and revoke certificates. This internal CA will work in conjunction with a Directory Server, used for managing the user's information and a Timestamp Server, for determining the existence of messages or files at a specific point of time. Figure I shows which elements are necessary to implement in the campus.

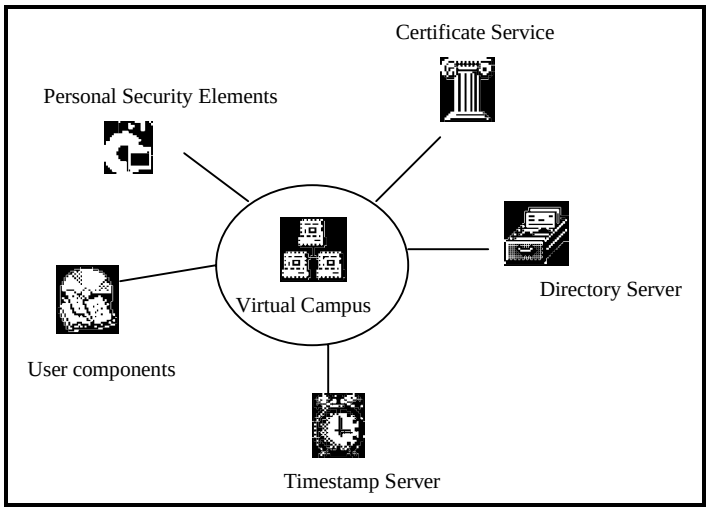

Figure I: PKI Components in a Virtual University

2.1. Elements of the virtual campus

A PKI consists of policies, services and professionals. A policy is a plan of action proposed or adopted by an entity. In the next sections we will show some helping questions for defining the policies of each service included in this model: Certificate, Directory and Timestamping Service. There are four classes of professionals involved: agents, administrators, designers and end-users. Agents are responsible that the interaction of the users with the services work, while administrators are responsible for auditing the services. Each service includes programs for the interaction of users, agents and administrators with the services. These programs are defined by the designers. Finally we have the end user, who uses every service according to his necessities. He interacts with every

program defined by the designer and with the servers included in the virtual campus. Students, teachers, tutors and any administration personal are included as end-users. The use of certificates within this paper will be seen from the end-user‘s point of view.
A PKI for a virtual university consists of these components:

2.1.1. Certificate Service

A Certificate Authority (CA) is the most important component of a PKI, because it is the entity that issues, manages and revokes certificates. Through the certificate service, users of an intranet can apply for certificates and obtain and install them in their computers. In the intranet of the university it is enough that the users trust this CA and the generated digital identifications.
In this server are included policies that rule each action that has to take place. The answer to a series of questions like the flowing, could help to define the policies of a Certificate Server:

- Issuing a certificate
  - ✓ where is the personal information of the user taken from?
  - ✓ is the personal data correct?
  - ✓ can this data be used for other purposes?
  - ✓ how will it be verified?
  - ✓ when is not possible to generate a certificate?
  - ✓ are all the users able to obtain one?
  - ✓ which validity period will it have?
  - ✓ how will the certificate be issued? Will the private key be generated when applying for it or at the moment that is generated?
  - ✓ where will the certificate be stored? Is it necessary to generate a new certificate if the user changes his workplace? Or can the certificate be exported? If so, will there be any provided mechanism?
- Managing certificates
  - ✓ are there any condition under which the use of these certificates is not possible?
  - ✓ can certificates be used to compute which resources are used, when and for how long?
  - ✓ in case of lost of a private key, are there any provided key recovery services within the PKI?
- Revoking a certificate
  - ✓ which professionals could revoke certificates?
  - ✓ where will be shown the control revocation lists (CRL)?

  A revocation [6] of a certificate might take place if the owner of it thinks that his private key has been compromised, because a change of name or likewise when a student finishes a career or study at the university. Users requesting the revocation of their certificates must sign the request and include their certificate within it. All revocation requests are sent to the CA, which verifies them and the certificates. If both are valid, the certificate’s details are added to the most recent Control Revocation List (CRL) and the CRL is signed by the CA. A system using certificates checks not only the certificate signature and validity but also checks that the serial number of the digital identification is not contained in the CRLs.

2.1.2. Directory Server

A directory service is a collection of software which is used to store information about the organisation. The goal of this service is to keep data of the university, so that it can be retrieved later when searching for all that information.
In a PKI a directory server can be used to store the data of the users obtaining and using certificates. This data includes all the user’s information such as:

- for a student
  - name;
  - student's ID;
  - career;
  - actual semester;
  - physical address: locality, state, country;
  - telephone number;
  - e-mail: address, server, preferences;
  - group: student.

- for a teacher
  - name;
  - teacher's ID;
  - subject;
  - salary;
  - physical address: locality, state, country;
  - telephone number: office, personal, handy;
  - e-mail: address, server, preferences;
  - group: teacher.

Some of the policies to be defined in this server could be the following:

- ✓ which information would be kept
- ✓ ways to access the directory
- ✓ ways of updating and managing the directory
- ✓ who has access to the directory and with which privileges

These two services: certificate and directory, could be used together to obtain digital identifications. Normally, people studying at a virtual university does not have big computer knowledge. They can interact with the computer but just as with another working tool. So the process of applying and obtaining a certificate, should be designed as simple as possible, with interfaces that are easy to use and letting the user give as little information as possible. For example when applying for a certificate, the user normally has to give a lot of information like locality, state, country, e-mail, ID, telephone number, etc. Users normally doubt how this information should be given. So it is better to ask them just for simple information like name and ID, and take all the other needed data from the information saved in the directory server. An example of this model could be read at [7].

2.1.3. Timestamp Server

A Timestamp Server is necessary when there is a need to determine the existence of a document at a particular point of time.

For example, there are many students that have to take examination today, and they could be in different places. As everyone has to have the same chances, all the examinations should be sent before and after an specific time, it is necessary to timestamp each document. The student Alice writes her examination, and signs it digitally using her valid installed certificate and sends it to the Timestamp Server (TS). The TS checks the signature to determine if it really belongs to Alice, and if so adds a timestamp to it and signs it. After that he sends it to Alice and to the examination group (EG). Each TS keeps a database with document, user and time. The EG receives the signed document from the TS, verifies the signature and obtain the examination of Alice, with the corresponding timestamp (Figure II).

In the policies of such a server should be defined if it is necessary to send the document itself or if it is enough to send a hash of it. In this way could be assured the confidentiality of the documents. Also the database of the TS would be smaller as it would only contain hash values instead of full documents.
This server can be used for [8]:

- having in a IP-net a trustworthy time server
- including the date and time in a digital stamp bound to any digital object
- producing a digital timestamp for any valid document sent by any valid client

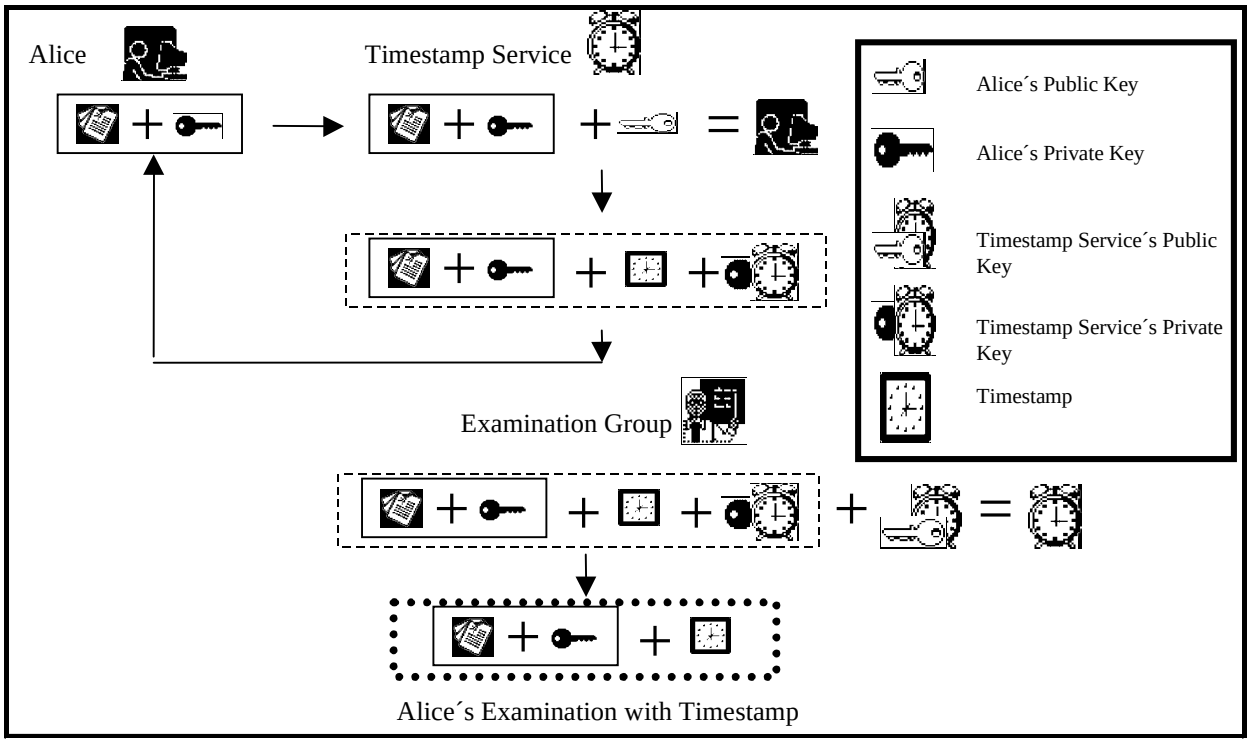

Figure II: Timestamp Procedure

2.1.4. Personal Security Elements

Smart cards, diskettes or just the hard disk can be used as personal security elements for storing private keys. They can be used as a way of backing up this data.

2.1.5. User components

In the user components are included the different elements or resources that are available in the campus for the user, like chats, newsgroups, e-mail, learning material. The tools necessary for applying, acquiring and using certificates are also part of this section.

2.2. Use of certificates

We will explain now the different uses that certificates will have within the virtual campus.

2.2.1. Authentication

When the user logs into the virtual campus he has to give username and password (basic authentication). And then sometimes for using each resource he also has to give passwords. This is

a problem for the user who has to remember several different passwords. From the security point of view, we know that all the information sent over a TCP/IP network passes through various computers until it reaches its destination. It could happen that an eavesdropper sees, changes or alters the data being sent. In the case of basic authentication, passwords (if not encrypted) are sent in clear over the network with the corresponding risks.
We propose the use of a single sign-on solution based on certificates (strong authentication) and on the Secure Socket Layer (SSL) protocol. This solution consists in authenticating only once to the server and then have access to all the resources without any additional passwords. The strong authentication is based in two facts: something the user has (a certificate) and something the user knows (the password that protects the private key). Although in this kind of authentication it is also needed a password (to gain access to the private key database), this does not mean a risk because the password is not send over the network. The private key is normally stored in the local computer.
Users in a virtual university are divided in groups, for example students, teachers, tutors and university's administration. Subgroups are also included to distinguish for example between students of different careers and/or different semesters. The Access Control Lists (ACLs) are used to determine which group has access to which resource and if authentication is needed and, if so, ask for it. Using the installed certificate of the user the server will be able to determine the user's identity and by using the directory server ascertain the group and if the access should be accepted or denied.
In summary the following are clear advantages for the users of this kind of authentication:

- the user has to remember only one password
- the password will not be sent over the network avoiding this way the security risks described above
- using his installed certificate he will have access to the virtual campus and all its resources

2.2.2. Digital signatures

The use of digital signatures helps to prove the origin of data (authentication), verify whether the data has been altered (integrity) and determine that the sender is really the one who sent the data (non-repudiation).
They can be used to determine:

- authorship of resources, exercises, books
- sender of e-mails
- applications for information
- subscription to newsgroups
- exchange of application forms, identity documents with the university's administration

The procedure for signing consists in giving the password that protects the private key's database and to use the private key to encrypt the data. The receiver just decrypts the data using the public key of the sender and in this way verifies the sender's signature.

2.2.3. Encryption of data

The encryption provides confidentiality in the communications, that is privacy in the messages and data. This could be important for:

- sending credit card numbers for paying the university's courses
- sending personal/private information to the university's administration
- using e-mail
- obtaining in a private way the results of exercises, examinations

- distribution of research results
- making personal data of students only available to authorised persons
- notification of private events to specific persons

For encrypting data using certificates, the sender uses the public key (stored in the certificate) of the receiver. It can also be combined with digital signatures in order to obtain its properties.

2.2.4. Timestamping files

The Timestamping can be used for doing partial examinations on-line where the teacher states the time of begin of an examination, and makes the exercises available to all the students. They all have to have the same chances: all receive the examination at the same time, they have the same amount of hours to finish them. Results send after the deadline will not be considered. How this works was defined in the example shown above in the Timestamp Server.

Other uses of timestamping inside a virtual university includes:

- deadlines for applications at the university's administration
- inscription in courses with limited number of students (i. e. only the first 20 who apply can do it).

3. Conclusion

This paper has presented the different components of a PKI to be integrated in a virtual university. We also propose the use of digital certificates for encrypting and signing the information, authenticating to the virtual campus and its resources and timestamping documents and files. The benefits of the use of PKI inside a virtual university are clear, it only needs to be studied how the interfaces for obtaining certificates and using them must be defined, so that end users will adequate themselves properly to this new tool.

4. References

[1] L. Carswell, ***The 'Virtual University': Toward an Internet paradigm?*** (6th Annual Conference on the Teaching of Computing, Dublin, Ireland, 1998).

[2] D. Casey, ***Learning "From" or "Through" the Web: Models of Web Based Education***. (6th Annual Conference on the Teaching of Computing, Dublin, Ireland, 1998).

[3] B. Schneier, ***Applied Cryptography***. (John Wiley & Sons, New York, 1996).

[4] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. , ***Handbook of Applied Cryptography***. (CRC Press, Florida, 1997).

[5] W. Diffie and M.E. Hellman, ***New Directions in Cryptography***. (IEEE Transactions on Information Theory, 1976).

[6] R. Housley, W. Ford und W. Polk, ***IETF RFC* 2459** (January 1999).

[7] M. Podestá, F. Losemann, T. Engel und C. Meinel, ***Design and Implementation of a Certificate Authority Front-End***. (DISC, México, 1999).

[8] J. Dávila Muro, L. Fincias**, *Diseño y realización de un Servicio de Sellado Digital de Tiempo***. CriptoLab – Facultad de Informática – Universidad Politécnica de Madrid, (Noviembre 1998) http://tirnanog.ls.fi.upm.es/CriptoLab/Biblioteca/Conferencias/JTRedIris98_mem.pdf